

7

الهاكر الأخلاقي

Viruses and Worms

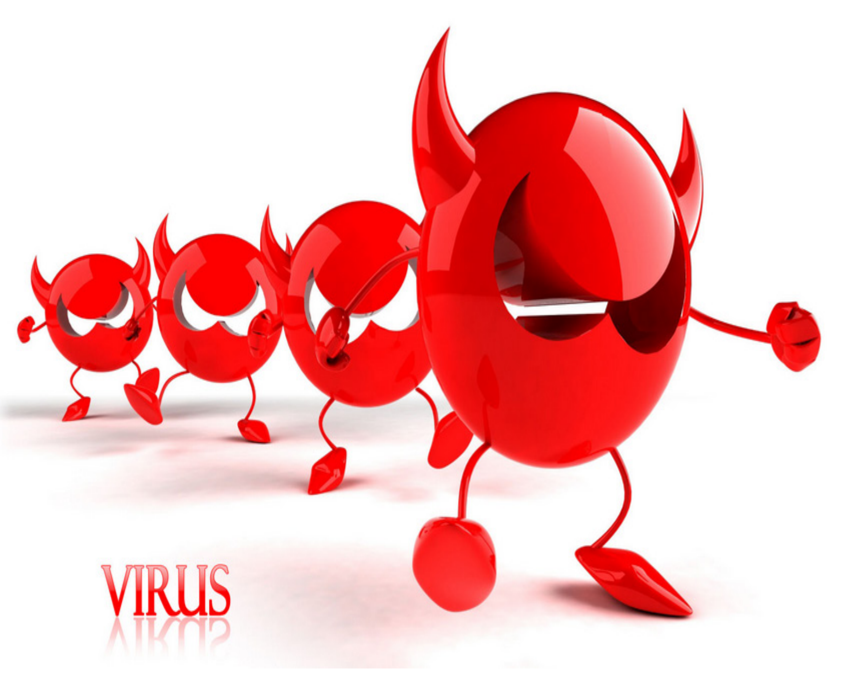
By

Dr.Mohammed Sobhy Teba
Virus and Worms
https://www.facebook.com/tibea2004

CONTENTS



الهدف من هذه الوحدة هو عرض مختلف الفيروسات والديدان(*worms*) المتاحة اليوم. فهو يوفر لك المعلومات عن كل الفيروسات والديدان المتاحة. يدرس هذه الوحدة طريقة عمل فيروس الكمبيوتر، وظيفتها، والتصنيف، والطريقة التي يؤثر بها على النظم. وهذه الوحدة تخوض في التفاصيل حول مختلف التدابير المضادة المتاحة للحماية ضد هذه العدوى من الفيروسات. الهدف الرئيسي من هذه الوحدة هو التثقيف عن الفيروسات المتاحة والديدان، ومؤشرات هجومهم وسبل الحماية ضد الفيروسات المختلفة، واختبار النظام الخاص بك أو الشبكة ضد الفيروسات أو وجود الديدان. وهذه الوحدة تعرفكم على الاتي:



- مقدمة عن الفيروسات
- مراحل حياة الفيروسات
- عمل الفيروسات
- المؤشرات على هجوم الفيروسات
- كيف احصل على جهاز كمبيوتر مصاب بالفيروسات؟
- تحليل الفيروسات
- أنواع الفيروسات
- صناعة الفيروسات
- صانع الديدان (**worms**)
- طرق تحليل البرامج الخبيثة
- خدمات تحليل البرامج الخبيثة عبر الإنترنت
- الفيروسات والديدان
- التدابير المضادة
- أدوات مكافحة الفيروسات
- اختبار الاختراق بالنسبة للفيروسات

Virus And Worms Concept 7.1 (مفهوم الفيروسات والديدان)

هذا القسم يقدم لك المعرفة حول العديد من الفيروسات والديدان المتاحة اليوم ويعطيك لمحة موجزة عن كل الفيروسات والإحصاءات من الفيروسات والديدان في السنوات الأخيرة. وهو يسرد الأنواع المختلفة من الفيروسات وآثارها على نظامك. العمل من الفيروسات في كل مرحلة وسيتم مناقشتها بالتفصيل. ويسلط الضوء على التقنيات المستخدمة من قبل المهاجم لتوزيع البرامج الضارة على شبكة الإنترنت.

مقدمة عن الفيروسات

فيروسات الكمبيوتر لديها القدرة على أن تعيث فسادا في كل من قطاع الأعمال وأجهزة الكمبيوتر الشخصية. في جميع أنحاء العالم، فان معظم الشركات قد أصيبت في مرحلة ما. الفيروس هو برنامج ذاتي تكرار التي تنتج التعليمات البرمجية الأكواد الخاصة به عن طريق ربط نسخ منه إلى اكواد أخرى قابلة للتنفيذ. يعمل هذا الفيروس دون علم أو رغبة المستخدم. مثل الفيروس الحقيقي، حيث ان فيروس كمبيوتر معدي ويمكنه أن يصيب غيره من الملفات. ومع ذلك، يمكن لهذه الفيروسات أن تصيب آلات الخارجية فقط بمساعدة من مستخدمي الكمبيوتر. بعض الفيروسات تؤثر على أجهزة الكمبيوتر بمجرد تنفيذ/تشغيل الأكواد الخاصة بهم؛ الفيروسات الأخرى تظل كامنة حتى يتحقق ظرف منطقي محدد سلفا. هناك ثلاث فئات من البرامج الخبيثة:

- **Trojans and rootkits**
- **Viruses**
- **Worms**

الديدان (**worms**) هي برامج خبيثة التي يمكنها أن تصيب كلا من الأجهزة المحلية والبعيدة. تنتشر الديدان تلقائيا عن طريق إصابة النظام بمجرد وجوده على الشبكة، وحتى يمكنه أن ينتشر إلى مزيد من الشبكات الأخرى. وبالتالي، فان الديدان لديها إمكانات كبيره للتسبب بالضرر لأنها لا تعتمد على إجراءات المستخدم لتنفيذها. وهناك أيضا برامج الخبيثة في الحقيقة تحتوي على كافة مميزات الأنواع الثلاثة لهذه البرامج الخبيثة والتي تعتبر اشرثهم.



الاحصائيات عن الفيروسات والديدان (Virus and Worm Statistics)

المصدر: http://www.av-test.org/en/home

التمثيل الرسومي التالي يعطي معلومات مفصلة عن الهجمات التي وقعت في السنوات الأخيرة. ووفقا للرسم البياني نجد أن **11,666,667** من الأنظمة فقط، قد أصيبوا من قبل الفيروسات والديدان في العام **2008**، في حين أنه في العام **2012**، زاد العدد الى **70 مليون** من النظم، وهذا يعني أن نمو الهجمات الخبيثة على الأنظمة يتزايد في كل سنة أضعافا مضاعفة عن السنوات السابقة.



دورة حياة الفيروس (Stage of Virus Life)

فيروسات الحاسبات الشخصية لها دورة حياة مثل الفيروسات التي تصيب الإنسان، وهذه الدورة تبدأ من تصميم الفيروس على حاسب الشخص الذي قام بتطويره، وتنتهي عندما تتم إزالته نهائيا من على الحاسبات الشخصية وشبكة الإنترنت بمختلف أنحاء العالم. وهناك ستة مراحل لدورة حياة فيروسات الكمبيوتر تتمثل فيما يلي:

1- مرحلة التصميم (Design):

عملية تصميم فيروس جديد تحتاج إلى شخص على درجة عالية من الكفاءة في التعامل مع لغات البرمجة على الحاسب الشخصي أو مجموعات البناء (*Construction kits*). يمكن لأي شخص لديه معرفة بلغات البرمجة الأساسية إنشاء الفيروسات.

2- النسخ/الانتشار (replication):

يقوم الفيروس أولا بالتكاثر داخل النظام المستهدف على مدى فترات من الزمن. عادة ما يقوم مطورو الفيروسات بنشر فيروساتهم على أكبر عدد من الحاسبات الشخصية قبل أن يبدأ الفيروس بإحداث الآثار التدميرية المكلف بها، السبب في ذلك هو نشر أكبر عدد من النسخ قبل أن تنتبه شركات مقاومة الفيروسات لوجوده فتضع البرامج المضادة له، في هذه المرحلة تصل الفيروسات إلى حاسبات وتظل بها دون أن تظهر أي أعراض على الحاسبات المصابة.

3- الإطلاق/النشاط (Lunch):

تبدأ الفيروسات في النشاط وإحداث الآثار التدميرية التي تم برمجتها للقيام بها عند وقوع حدث معين. قد يتم برمجة الفيروس لكي ينشط في توقيت معين أو عند تشغيل برنامج ما أو عند الاتصال بشبكة الإنترنت أو عند وصول جزء ثاني من الفيروس إلى الحاسب المصاب، الآثار التدميرية تتنوع من تدمير ملفات مخزنه على الحاسب أو استهلاك المساحات الخالية في وحدة التخزين أو إلغاء برامج أو سرقة معلومات.

4- اكتشاف الفيروس (Detection):

يتم التعرف على الفيروس على أنهه تهديدات تقوم بإصابة الأنظمة المستهدفة. قد لا تتبع هذه الخطوة دائما عملية نشاط الفيروس، فقد تكون الشركات المنتجة لبرامج مقاومة الفيروسات أكثر ذكاء، بحيث تكتشف وجود الفيروس قبل أن ينشط.

عندما يتم اكتشاف أي فيروس جديد يتم إبلاغ هيئة تسمى **icse** في واشنطن بالولايات المتحدة بنوعية هذا الفيروس وطبيعته، لكي يتم توثيق هذه المعلومات وإرسالها إلى كل الشركات المنتجة لبرامج مقاومة الفيروسات.

5- المواجهة/التأسيس (Incorporation):

في هذه المرحلة تقوم شركات إنتاج برامج مقاومة الفيروسات بتعديل برامجها وملفاتها لكي تتعامل مع الفيروس الجديد. ولكل فيروس بصمة خاصة به (هي الكود الذي تكتب به أوامر الفيروس بأحد لغات الحاسب)، ويتم إضافة هذه البصمة لملفات البرامج. يقوم المستخدمين بتنزيل الملفات بعد التعديل من على موقع الشركة على شبكة الإنترنت، ويقومون بتحديث برامج المقاومة به، هذه المرحلة قد تصل إلى ستة أشهر حسب نوع الفيروس.

6- الاستئصال/الإزالة (Elimination):

بعد فترة من قيام عدد كبير من المستخدمين بتحديث برامجهم لمقاومة الفيروس بالتعديلات التي تكتشف وتقضى على الفيروس، تنحسر آثار هذا الفيروس بحيث تنخفض درجة تهديده لمجتمع المعلومات العالمي. لم يتم التأكد حتى الآن من أن أحد فيروسات الحاسبات قد تم القضاء عليه تماما بحيث لا يوجد على أي حاسب شخصي في العالم، ولكن مئات الفيروسات تم الحد من خطورتها ومحاصرتها إلى حد كبير، بحيث لم تعد تشكل أي تهديد في الوقت الحالي لمستخدمي الحاسبات الشخصية أو الخادمة.

طريقة عمل الفيروسات: مرحلة العدوى — Working of Viruses: Infection Phase

الفيروسات تهاجم النظام المضيف الهدف باستخدام أساليب مختلفة. حيث أنها تقوم بلصق نفسها بالبرامج ونقل نفسها إلى برامج أخرى من خلال الاستفادة من بعض الأحداث. الفيروسات تحتاج إلى مثل هذه الأحداث لتأخذ مكان لها لأنها لا يمكن أن:

- تبدأ ذاتيا (Self-start)
- تصيب الأجهزة الأخرى (Infect other hardware)
- تسبب الأضرار المادية إلى كمبيوتر (Cause physical damage to a computer)
- تنقل نفسها باستخدام ملفات غير قابلة للتنفيذ (Transmit themselves using non-executable files)

عموما عمل الفيروسات ينقسم إلى مرحلتين، مرحلة العدوى ومرحلة الهجوم.

في مرحلة العدوى(Infection phase)، الفيروس ينسخ نفسه ثم يقوم بربط اكواده الى الملف القابل للتنفيذ (**.exe**) في النظام. الان البرامج التي تم تعديلها نتيجة العدوى بالفيروس تقوم بتمكين وظائف الفيروس لتشغيلها على هذا النظام. الفيروس يصبح جاهزا للعمل بمجرد تشغيل البرنامج المصاب بالفيروس، حيث ان اكواد البرامج تؤدى الى اكواد الفيروسات. مطوري الفيروسات لديه بعض التحفظات للحفاظ على التوازن بين عوامل عده مثل:

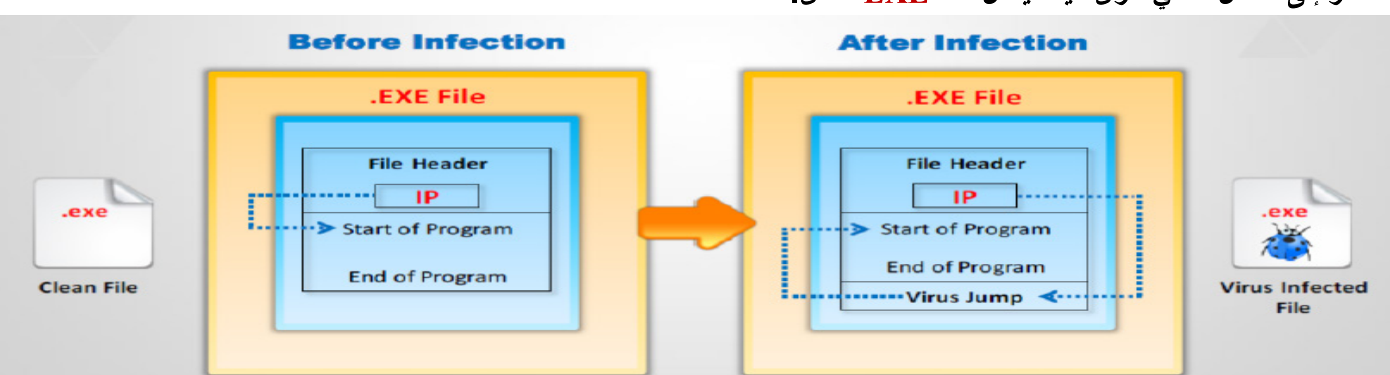
- كيف سوف يصيب الفيروس؟
- كيف سوف ينتشر هذا الفيروس؟
- كيف سوف يقيم في ذاكرة الكمبيوتر الهدف من دون أن يتم اكتشافه؟

من الواضح، أن الفيروسات يمكن تشغيلها وتنفيذها لكي تقوم بوظيفة ما. هناك العديد من الطرق لتنفيذ البرامج عندما يكون جهاز الكمبيوتر في وضع العمل. على سبيل المثال، حيث عندما يتم تثبيت أي من البرامج فانه سوف يستدعى العديد من البرامج الأخرى التي تم إنشائها

واصبحت من صلب النظام(**built into a system**) ، وبعض من هذه البرامج متوسطة التوزيع. وبالتالي، فإذا كان برنامج الفيروس موجود بالفعل، فإنه يمكن تفعيلها مع هذا النوع من التنفيذ (*execution*)وإصابته العديد من البرامج المثبتة الاضافية كذلك.

يبدأ الفيروس دورة حياته على الجهاز بشكل مشابه لبرنامج حصان طروادة، فهو يختبئ في ثنايا برنامج أو ملف آخر، وينشط معه. في الملفات التنفيذية الملوثة، يكون الفيروس قد أضاف اكواده إلى البرنامج الأصلي، وعدل تعليماته بحيث ينتقل التنفيذ إلى اكواد الفيروس. وعند تشغيل الملف التنفيذي المصاب، يقفز البرنامج عادة إلى تعليمات الفيروس، فينفذها، ثم يعود ثانية لتنفيذ تعليمات البرنامج الأصلي. وعند هذه النقطة يكون الفيروس ناشطاً، وجهازك أصبح ملوثاً. وقد ينفذ الفيروس مهمته فور تنشيطه (ويطلق عليه فيروس العمل المباشر (*direct-action*)، أو هناك البعض الاخر لا يصيب الجهاز بمجرد تنفيذها بل يقبع منتظراً في الذاكرة منتظرا حدثا معينا، باستخدام وظيفة "الإنهاء والبقاء في الذاكرة" (**terminate and stay resident**،**TSR**)، التي تؤمنها نظم التشغيل عادة. وبالتالي، من الصعب أن يتم التعرف عليه وتنتمي غالبية الفيروسات لهذه الفئة، ويطلق عليها الفيروسات "المقيمة". ونظراً للإمكانيات الكبيرة المتاحة للبرامج المقيمة في الذاكرة، بدءاً من تشغيل التطبيقات والنسخ الاحتياطي للملفات إلى مراقبة ضغطات لوحة المفاتيح ونقرات الماوس (والكثير من الأعمال الأخرى)، فيمكن برمجة الفيروس المقيم، لتنفيذ أي عمل يمكن أن يقوم به نظام التشغيل، تقريباً. يمكن تشغيل الفيروس المقيم كقنبلة، فيبدأ مهمته على جهازك عند حدث معين. ومن الأمور التي تستطيع الفيروسات المقيمة عملها، فحص (**scan**) قرصك الصلب وأقراص الشبكة بحثاً عن الملفات التنفيذية، ثم نسخ نفسها إلى هذه الملفات وتلويثها.

فلننظر إلى الشكل التالي لنرى كيف يعمل ملفEXE معدى.



في هذا الشكل، حيث نجد أن رأس ملفEXE ، عندما يتم تشغيله، فإنها تبدأ تشغيل التطبيق. ولكن بمجرد إصابة هذا الملف، فانه يذهب أولا الى التعليمات الخاصة بأكواد الفيروس لتشغيلها أولا ثم ينتقل الى اكواد التطبيق المراد تشغيله.

- يقوم الفيروس بإصابة الملفات عن طريق ربط نفسه إلى برنامج تطبيق قابل للتنفيذ. الملفات النصية مثل **source code**، ملفات **patches** وملفات الاسكريبت، وما إلى ذلك، تعتبر أهدافا محتملة للعدوى بالفيروس.
- فيروسات قطاع التشغيل (*Boot Sector Virus*) تقوم بتنفيذ الأكواد الخاصة بها في المقام الأول قبل أن يتم تشغيل الكمبيوتر الهدف وهو من أخطر أنواع الفيروسات حيث انه من الممكن أن يمنعك من تشغيل الجهاز.

في مرحلة الهجوم (Attack phase)، بمجرد أن تقوم الفيروسات بالانتشار في جميع أنحاء النظام الهدف، فإنها تبدأ بإفساد الملفات والبرامج في النظام المضيف. بعض الفيروسات تحتاج الى بعض الاحداث والتي تعتبر الزناد للتنشيط لإفساد النظام المضيف. بعض الفيروسات لها **bugs** والتي تكرر نفسها، والقيام ببعض الأنشطة مثل حذف الملفات وزيادة وقت الدورة.

حيث أنها تقوم بإفساد الأهداف فقط بعد نشرها على النحو المنشود من قبل المطورين. معظم الفيروسات التي تهاجم الأنظمة الهدف تقوم بتنفيذ إجراءات مثل الاتي:

- حذف الملفات وتغيير المحتويات في ملفات البيانات، وبالتالي تسبب إبطاء النظام.
- أداء بعض المهام ليس لها علاقة بالتطبيقات، مثل تشغيل الموسيقى وإنشاء الرسوم المتحركة.

Unfragmented File Before Attack

File: A — File: B

Page: 1 | Page: 2 | Page: 3 | Page: 1 | Page: 2 | Page: 3

File Fragmented Due to Virus Attack

Page: 1 File: A | Page: 3 File: B | Page: 1 File: B | Page: 3 File: A | Page: 2 File: B | Page: 2 File: A

بالرجوع إلى هذه الصورة السابقة، فنجد أننا عندنا اثنين من الملفات A و B. في المقطع الأول، نجد أن الملفين يقعوا واحدا تلو الآخر بطريقة منظمة. بمجرد قيام اكواد الفيروس بإصابة الملف، فإنه يقوم بتغير مواقع الملفات التي تم وضعها على التوالي، مما يؤدي إلى عدم الدقة في تخصيص مواقع الملفات، والتي تسبب إبطاء النظام عند محاولة المستخدمين استرجاع ملفاتهم. في هذه المرحلة:

- الفيروسات تعمل عندما يتم تشغيل بعض الأحداث.
- بعضها يعتمد في تشغيله وافساده عبر أخطاء (**BUGS**) البرامج المدمجة بعد تخزينه في الذاكرة المضيف
- تتم كتابة معظم الفيروسات لإخفاء وجودها، والهجوم يبدا بعد ان تنتشر في المضيف إلى أقصى حد.

لماذا يلجا الناس الى إنشاء فيروسات الكمبيوتر؟

فيروسات الكمبيوتر لا تولد ذاتيا، ولكن يتم إنشاؤها من قبل العقول السيبرانية الجنائية(***cyber-criminal***) ، مصممة عمدا لتتسبب في الحوادث المدمرة في النظام. عموما، يتم إنشاء الفيروسات مع وجود دافع سيء السمعة. مجرمي الإنترنت ينشؤا الفيروسات لتدمير البيانات في الشركة، كعمل من أعمال التخريب أو المزحة، أو لتدمير منتجات الشركة. ومع ذلك، في بعض الحالات، فان المقصود من الفيروسات في الواقع أن تكون جيدة للنظام. وقد صممت هذه لتحسين أداء النظام عن طريق حذف الفيروسات المدمجة سابقا في الملفات.

فيما يلي بعض الأسباب التي أدت الى كتابة الفيروسات وتشمل الاتي:

- إلحاق الضرر بالمنافسين inflict damage to competitors
- مشاريع بحثية Research projects
- المزح Pranks
- التخريب Vandalism
- مهاجمة منتجات شركات محددة Attack the products of specific companies
- توزيع رسائل سياسية Distribute political messages
- تحقيق مكاسب مالية Financial gain
- سرقة الهوية Identity theft
- برامج التجسس Spyware
- الابتزاز Cryptoviral extortion

المؤشرات على هجمات الفيروسات

الفيروس الفعالة تميل إلى أن تتكاثر بسرعة ويمكن أن تصيب عددا من الآلات في غضون ثلاثة إلى خمسة أيام. يمكن للفيروسات أن تصيب ملفات **Word** والتي عند نقلها، يمكن أن تصيب أجهزة المستخدمين الذين يحصلون عليها. ويمكن للفيروس أيضا الاستفادة من خوادم الملفات من أجل أن تصيب الملفات. وفيما يلي مؤشرات على وجود هجوم الفيروس على نظام الكمبيوتر:

- البرامج تستغرق وقتا أطول للتحميل.
- القرص الصلب دائما ممتلئ لا يحتوي على مساحة فارغه، حتى من دون تثبيت أي من البرامج.
- محرك الأقراص المرنة (***Floppy disk***) أو القرص الصلب تجده يعمل حتى في أوقات عدم استخدامه.
- ملفات مجهولة تحافظ على الظهور على النظام.
- لوحة المفاتيح أو الكمبيوتر تبعث أصوات غريبة أو التصفير.
- شاشة الكمبيوتر يعرض رسومات غريبة.
- تحويل أسماء الملفات الى أسماء غريبة، وغالبا ما يصعب التعرف عليها.
- يصبح القرص الصلب لا يمكن الوصول إليه عند محاولة التشغيل من محرك أقراص مرنة (**Floppy disk – CDROM**)
- حجم البرامج يتغير باستمرار.
- الذاكرة على النظام تبدو قيد الاستخدام والنظام بطيء.

كيف يصبح جهاز الكمبيوتر مصابا بالفيروسات؟

هناك العديد من الطرق التي يصاب بها جهاز كمبيوتر عن طريق الفيروسات. الأساليب الأكثر شعبية هي على النحو التالي:

- عندما يقبل المستخدمين الملفات والتنزيلات دون التحقق بشكل صحيح من المصدر.
- المهاجمون عادة يقومون بإرسال الملفات المصابة بالفيروسات كمرفقات للبريد الإلكتروني لنشر الفيروسات على نظام الضحية. إذا فتح الضحية البريد، فان الفيروس يصيب النظام تلقائيا.
- المهاجمين يقومون بدمج الفيروسات في البرامج الشعبية وتحميل البرمجيات المصابة على مواقع تهدف إلى تحميل البرمجيات. عندما يقوم الضحية بتحميل البرامج المصابة وتثبيته، فان النظام يصاب.
- فشل في تثبيت إصدارات جديدة أو تحديث مع أحدث **Patch** والتي تهدف إلى إصلاح الأخطاء المعروفة قد يعرض النظام للفيروسات.
- مع التكنولوجيا المتزايدة، فان المهاجمون أيضا تقوم بتصميم فيروسات جديدة. الفشل في استخدام أحدث التطبيقات لمكافحة الفيروسات قد يعرضك لهجمات الفيروسات.

التقنيات الأكثر شعبيه والتي تستخدم لتوزيع البرامج الضارة على الإنترنت

المصدر: Security Threat Report 2012 (http://www.sophos.com/en-us.aspx)

- **Blackhat Search Engine Optimization (SEO)**: باستخدام هذه التقنية يقوم المهاجم بتعلية مرتبة الصفحات الخبيثة الى درجه عالية في نتائج البحث.
- **Social Engineered Click-jacking**: المهاجمين يقومون بخداع المستخدمين بالنقر على صفحات الويب التي تظهر وكأنها بريئة وسليمة المظهر ولكنها في الواقع تحتوي على البرمجيات الخبيثة.
- **Spearphishing Sites**: يتم استخدام هذه التقنية لمحاكاة المؤسسات الشرعية، مثل البنوك، في محاولة لسرقة بيانات دخول الحساب
- **Malvertising**: حيث يتم تضمين البرمجيات الخبيثة في الشبكة الإعلانية (**AD network**) التي تعرض عبر مئات المواقع المشروعة، وذات حركة المرور العالية.
- **Compromised Legitimate Websites**: المضيفين يستضيفون البرمجيات الخبيثة والتي تنتشر عبر الزوار الغافلين.
- **Drive-by Downloads**: المهاجم يستغل بعض الثغرات في برنامج المتصفح لتثبيت البرامج ضارة فقط من خلال زيارة الصفحة على شبكة الإنترنت.

Virus Hoaxes and Fake Antiviruses

Virus Hoaxes

تعني كلمة **Hoax** باللغة الإنجليزية خدعة أو حيلة وكذبة أو مكيدة، إذا **Virus hoax** يقصد به أكاذيب الفيروسات. الفيروسات، بحكم طبيعتها، قد خلقت انطباعا بانها مرعبة. **Hoaxes** عادة عباره عن رسائل بريدية التي تحتوي على تحذيرات عن فيروس ما، ترسل من قبل شخص ما (أو أكثر) بهدف إشاعة هذه الكذبة أو الـ **Hoax**، ومن ثم يتناقلها الآخرون بحسن نية معتقدين أنهم يخدمون أصدقاءهم بإرسال نفس التحذير لهم بعمل **forwarding** للرسالة الأصلية. في وقت قصير تنتشر هذه الرسالة في أنحاء الكرة الأرضية، وما هي في واقع الأمر سوى حيلة أو كذبة "هوكس". إن فيروس الكمبيوتر ما هو إلا برنامج صمم لإدراج نفسه في ملف يحتوي على برنامج آخر. وعندما يشتغل البرنامج الثاني، يصبح الفيروس نشطا، وعلى الأرجح مسببا مشكلة. فيروس الكمبيوتر، طبعا ممكن أن يكون مشكلة. ولكن، هنالك فيروسات حقيقية قليلة نسبيا، ولسوء الحظ، هنالك الكثير من الناس ينشرون إشاعات ليس لها أساس من الصحة عن الفيروسات، وخصوصا ما يسمى بفيروسات البريد الإلكتروني. عليك ألا تنخدع. في المرة التالية التي تحصل على أحد تحذيرات الفيروسات هذه، توقف عن إرساله لأصدقائك.

Virus hoax هي إنذارات كاذبة تزعم تقارير حول فيروسات غير موجودة.

- رسائل التحذير هذه، والتي يمكن نشرها بسرعة، والتي تشير إلى عدم فتح رسائل بريد إلكتروني معينة، والتي من شأنها أن تلحق الضرر بذلك النظام.
- في بعض الحالات، رسائل التحذير هذه أنفسها تحتوي على مرفقات الفيروس.
- تمتلك هذه القدرة على تدمير واسعة على الأنظمة الهدف.

العديد من **Hoaxes** تحاول "بيع" الأشياء التي هي من الناحية الفنية هراء. ومع ذلك، فإن **Hoaxer** (منشئ **Hoaxes**) يجب أن يكونوا نوعا ما خبراء لنشر **Hoaxes** بطريقه تجنبها من تحديدها والقبض عليها.
وبالتالي، فإنه من الجيد البحث عن التفاصيل التقنية حول كيفية أن تصبح مصابا. أيضا البحث عن المعلومات في البرية لمعرفة المزيد عن **Hoaxes**، وخاصة عن طريق فحص لوحات الإعلانات حيث يقوم الناس بمناقشة الأحداث الجارية في المجتمع.
حاول **crosscheck (الفحص)** للتعرف على هوية الشخص الذي يقوم بنشر التحذير. تطلع أيضا لمزيد من المعلومات حول **Hoax/التحذير** من المصادر الثانوية. قبل القفز إلى استنتاجات من خلال قراءة بعض الوثائق على شبكة الإنترنت، فيجب التحقق مما يلي:

- ما إذا تم نشر هذه الوثائق من قبل مجموعات الأخبار المشبوهة، فقم بفحص (**crosscheck**) المعلومات مع مصدر آخر.
- ما إذا كان الشخص الذي نشر الخبر هو ليس شخص معروف في المجتمع أو خبير، فقم بفحص (**crosscheck**) المعلومات مع مصدر آخر.
- ما إذا كانت جهة حكومية قامت بنشر هذه الأخبار، وينبغي أن يملك النشر أيضا إشارة إلى تنظيم فيدرالي مقابل له
- واحدة من الفحوصات الأكثر فعالية هو البحث عن **hoax virus** المشبوهة عن طريق الاسم الموجود في مواقع برامج الحماية من الفيروسات
- إذا كان النشر هو تقني، فابحث عن المواقع التي من شأنها أن تلبي الجوانب التقنية، وحاول توثيق هذه المعلومات.

Subject: FORWARD THIS WARNING AMONG FRIENDS, FAMILY AND CONTACTS

PLEASE FORWARD THIS WARNING AMONG FRIENDS, FAMILY AND CONTACTS! You should be alert during the next few days. Do not open any message with an attachment entitled 'POSTCARD FROM BEJING' or 'RESIGNATION OF BARACK OBAMA', regardless of who sent it to you. It is a virus that opens A POSTCARD IMAGE, then 'burns' the whole hard C disc of your computer.

This is the worst virus announced by CNN last evening. It has been classified by Microsoft as the most destructive virus ever. The virus was discovered by McAfee yesterday, and there is no repair yet for this kind of virus.

This virus simply destroys the Zero Sector of the Hard Disc, where the vital information is kept.

COPY THIS E-MAIL, AND SEND IT TO YOUR FRIENDS. REMEMBER: IF YOU SEND IT TO THEM, YOU WILL BENEFIT ALL OF US.

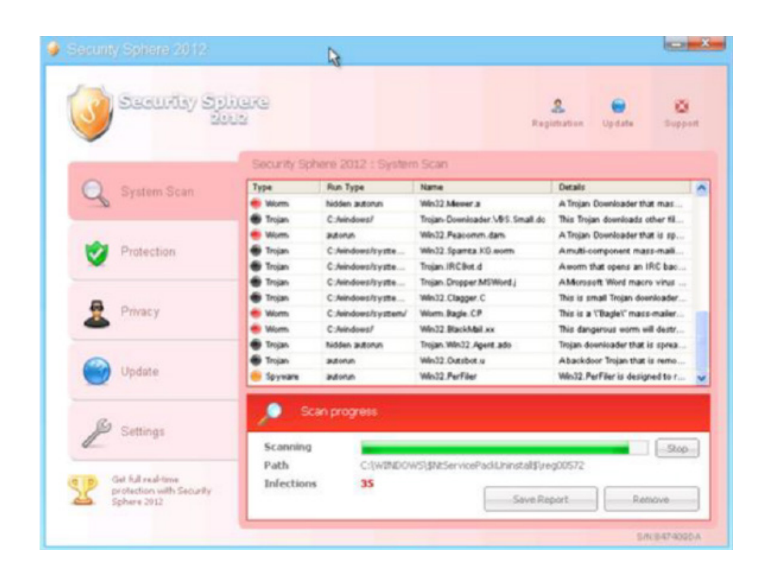
End-of-mail
Thanks.

Fake Antiviruses

Fake antivirus's هو وسيلة تؤثر على النظام من قبل القراصنة والتي يمكنها ان تسميم النظام وتفشى(**outbreak**) ملفات **registry** والنظام للسماح للمهاجم بالسيطرة الكاملة والوصول إلى جهاز الكمبيوتر الخاص بك. يبدو حيث انها تعمل على نحو مماثل لبرنامج مكافحة الفيروسات الحقيقية.
يبدو أن برامج مكافحة الفيروسات الوهمية تظهر أولا على مختلف المتصفحات ويقوم بتحذير المستخدمين بأن لديهم تهديدات أمنية المختلفة على النظام الخاص بهم، وتدعوهم من قبل هذه الرسالة المشبوهة بالفيروسات الحقيقية. عندما يحاول المستخدم إزالة الفيروسات، فانه يتم نقله إلى صفحة أخرى حيث يحتاج إلى شراء أو الاشتراك في مكافح الفيروس ذلك، والشروع في تفاصيل الدفع. برامج مكافحة الفيروسات الوهمية هذه تكون ملفقه بطريقه مثل التي تلفت انتباه المستخدم ليطمئن من تثبيت البرنامج.

بعض من الأساليب المستخدمة لتوسيع استخدام وتركيب برامج مكافحة الفيروسات الوهمية كما يلي:

- **Email and messaging**: المهاجمون يستخدموا البريد الإلكتروني والبريد المزعج والرسائل والشبكات الاجتماعية لنشر هذا النوع من البريد الإلكتروني المصابة إلى المستخدمين وتحفز المستخدم لفتح المرفقات لتثبيت البرامج.
- **Search engine optimization**: المهاجمين يقوموا بإنشاء صفحات تتعلق بمصطلحات البحث العامة أو الحالية وزرعها لتبدو وكأنها غير عادية وآخر في نتائج محرك البحث. تظهر صفحات الويب تنبيهات حول الإصابة التي تشجع المستخدم لشراء برامج مكافحة الفيروسات الوهمية.
- **Compromised websites**: المهاجمين يقومون بكسر المواقع ذات الشعبية سرا لتثبيت برامج مكافحة الفيروسات الوهمية، والتي يمكن استخدامها لجذب المستخدمين لتحميل برامج مكافحة الفيروسات الوهمية من خلال الاعتماد على شعبية الموقع.



Virus Analysis: DNSChanger

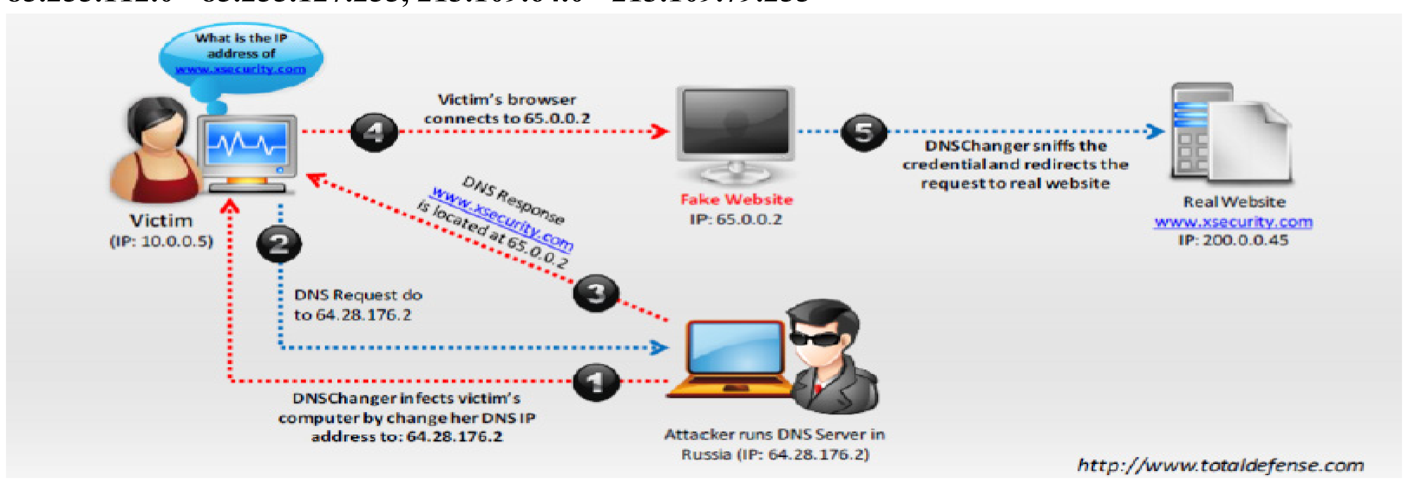
المصدر: http://www.totaldefense.com

DNSChanger (Alureon) هي برامج ضارة تنتشر من خلال رسائل البريد الإلكتروني، وحيل الهندسة الاجتماعية، والتنزيلات الغير موثوق بها من الإنترنت. انها بمثابة **bot** ويمكن تنصيفها على انها **botnet** والتحكم من مكان بعيد. هذه البرامج الضارة تقوم بإعادة توجيه **DNS**عن طريق تعديل إعدادات مفتاح **registry** ضد واجهة الجهاز مثل بطاقة الشبكة.

تلقت **DNSChanger** اهتماما كبيرا نظرا لوجود عدد كبير من الأنظمة المتأثرة في جميع أنحاء العالم، وحقيقة أنها جزء من الخدمة **botnet**، اتخذ مكتب التحقيقات الفيدرالي **(FBI)**التحقق من خوادم **DNS** المارقة/الخبيثة/المصابة لضمان ان المتضرر منها لم يفقد على الفور القدرة على ترجمة أسماء **DNS**. حيث ان **DNSChanger** حتى يمكنه تعديل إعدادات **DNS** على جهاز الضحية لتحويل حركة الإنترنت إلى المواقع الخبيثة من أجل توليد العائدات الإعلانية الاحتيالية، وبيع خدمات وهمية، أو سرقة المعلومات المالية الشخصية.

خوادم DNS المارقة/الخبيثة/المصابة تكون موجودة في النطاقات التالية:

64.28.176.0 - 64.28.191.255, 67.210.0.0 - 67.210.15.255
77.67.83.0 - 77.67.83.255, 93.188.160.0 - 93.188.167.255
85.255.112.0 - 85.255.127.255, 213.109.64.0 - 213.109.79.255



لإصابة النظام وسرقة وثائق التفويض، فان المهاجم يقوم أولا بتشغيل **DNS server**. حيث في هذا المثال نجد ان المهاجم يدير **DNSserver** الخاص به من روسيا مع **IP**، **64.28.176.2**. تاليا، يقوم المهاجم بإصابة جهاز الكمبيوتر الضحية عن طريق تغيير عنوان **IP** لـ **DNS** له إلى: **64.28.176.2**. عند تقوم البرمجيات الخبيثة هذه بإصابة النظام، فإنه يغير تماما إعدادات **DNS** للجهاز المصاب ويجبر جميع طلبات **DNS** بالذهاب إلى **DNSserver** الذي يعمل بواسطة المهاجم. بعد تغيير إعداد من **DNS**، فيتم إرسال أي طلب من قبل النظام لخادم **DNS** الخبيث. هنا، أرسلت الضحية طلب **DNS** " ما هوا عنوان **IP** لـ **www.xsecurity.com**" إلى

(64.28.176.2). يعطى المهاجم استجابة للطلب حيث يقول ان **www.xsecurity.com**، يقع في العنوان **65.0.0.2**. عندما يتصل المتصفح الضحية بال **65.0.0.2**، فإنه يتم توجيهه الى موقع على شبكة الانترنت وهمي تم إنشاؤها من قبل المهاجم مع عنوان **IP** **65.0.0.2**. **DNSChanger** يقوم بالتجسس على وثائق التفويض (اسم المستخدم وكلمات السر) وإعادة توجيه الطلب إلى الموقع الحقيقي (**www.xsecurity.com**) مع عنوان **IP 200.0.0.45**.

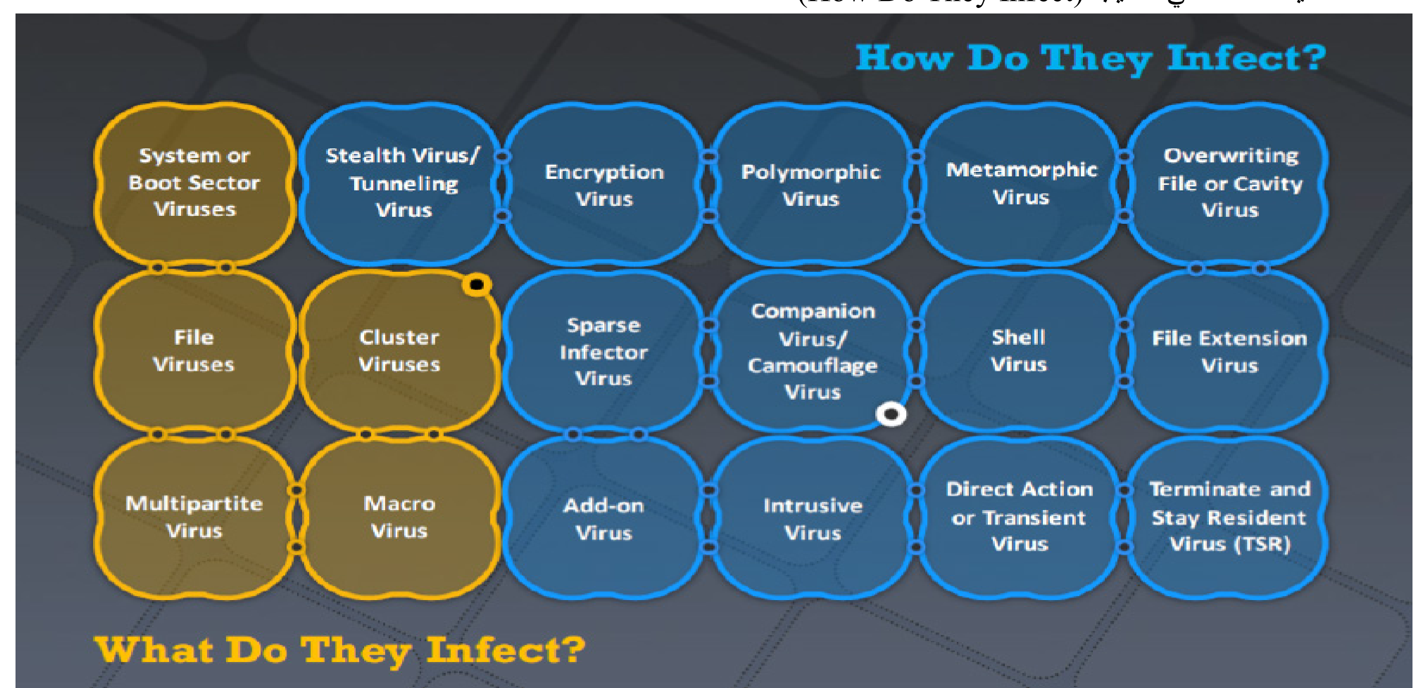
7.2 أنواع الفيروسات (Type of Viruses)

حتى الآن، لقد ناقشنا مختلف المفاهيم عن الفيروسات والديدان. الآن سوف نناقش الأنواع مختلفة من الفيروسات. يبرز هذا القسم الأنواع المختلفة من الفيروسات والديدان مثل فيروسات متعددة الملفات وفيروسات الماكرو والفيروسات العنقودية وفيروسات الشبح/نفق، وفيروسات التشفير والفيروسات المتحولة، وفيروسات الشل، وهلم جرا. فيروسات الكمبيوتر هي برامج خبيثة كتبها المهاجمين للدخول الى نظام استهدف عمدا دون الحصول على إذن المستخدم. ونتيجة لذلك، فإنها تؤثر على الجهاز الأمني وأداء الجهاز. نناقش هنا عدد قليل من الأنواع الأكثر شيوعا من فيروسات الكمبيوتر التي تؤثر سلبا على أنظمة الأمن بالتفاصيل على الشرائح التالية.

أنواع الفيروسات (Type of Viruses)

يتم تصنيف الفيروسات اعتمادا على فئتين:

- ما الذي تفعله لكي تصيب (What Do They Infect)؟
- كيف تفعله لكي تصيب (How Do They Infect)؟



What Do They Infect؟

- **فيروسات قطاع التشغيل (System/Boot Sector Virus):**

تعتبر من أقدم الفيروسات المعروفة لدى المستخدمين حيث تستطيع ان تصيب القرص الصلب والأقراص اللينة وتنتشر عن طريقها من مستخدم الى آخر وتكمن خطورة هذا النوع من الفيروسات في قدرتها على اصابة جزء أساسي من أي قرص صلب أولين حيث أن الأهداف الأكثر شيوعا للفيروس هي قطاعات النظام(*system sector*) ، والتي ليست سوى قطاعات **Master boot Record (MBR)** وقطاعات **DOS Boot Record System**. وهو الجزء المخصص لتوجيه الجهاز في كيفية تحميل برنامج نظام التشغيل ويقوم هذا الفيروس بتحميل نفسه للذاكرة في كل مرة يتم فيها تشغيل الجهاز. وهو من أخطر أنواع الفيروسات حيث انه يمنعك من تشغيل الجهاز. على سبيل المثال: **Disk Killer** و**Stone virus**.

- **فيروسات الملفات (File Virus):**

هذا النوع من الفيروسات يلحق نفسه كملف في أي برنامج تنفيذي ويتميز هذا النوع من الفيروسات بقدرته على الانتشار بعدة طرق وبسرعة مهولة منها الأقراص اللينة والأقراص المدمجة ورسائل البريد الإلكتروني كملف ملحق كما يمكنه الانتقال من البرامج المجانية والمتوفرة في الإنترنت وتكمن خطورته في قدرته على الانتشار السريع واصابة بقية الملفات الموجودة في البرامج التنفيذية الأخرى. فيروسات الملف أكبر من حيث العدد، ولكنها ليست هي الأكثر شيوعا. أنها تصيب عن طريق مجموعة متنوعة من الطرق، ويمكن العثور عليها في عدد كبير من أنواع الملفات.

- **فيروسات متعددة الملفات (Multipartite Virus):**

فيروس يقوم على دمج قدرات نوعين مختلفين من الفيروسات فيروسات الـ **boot sector** وفيروسات الملفات فتقوم هذه الفيروسات بإصابة جزء من ملفات النظام (مثل **programs file**)، وهذا الملفات بدورها تؤثر على قطاعات التمهيد ثم تتوزع لتنتشر على كافة أرجاء النظام. وكنتيجة لقدرات هذا الفيروس فإنه من الصعب جداً التخلص منه. مثل **Invader**، **Flip**، و**Tequila**.

- **الفيروسات العنقودية (Cluster Virus):**

Cluster virus's تصيب الملفات دون تغيير الملف أو زرع ملفات إضافية؛ حيث يقوم بتعديل معلومات **directory table** بحيث عند تشغيل تطبيق ما فانه يجعل نقطة الإدخالات تشير إلى رمز الفيروس بدلا من البرنامج الفعلي فيتم تحميل الفيروس بدلا من البرنامج وبالتالي يظهر للمستخدم بأن الفيروس قد أصاب كل الملفات. هذا الفيروس يصيب برنامجاً واحداً فقط في النظام ولكن ما يظهر للمستخدم هو أن جميع البرامج قد تمت إصابتها بالفيروس.

ملحوظه: Directory table هو جدول موجود في MBR حيث يسجل فيه الملفات والمجلدات الموجودة على النظام وموقعه على القرص الصلب.

- **فيروسات الماكرو (Macro Virus):**

ملفات ورد (**windows word**) او التطبيقات المشابه يمكنها أن تصاب من خلال فيروسات الكمبيوتر والتي تسمى فيروس ماكرو، الذي يؤدي تلقائيا سلسلة من الإجراءات عندما يتم تشغيل التطبيق أو أي شيء آخر. فيروسات الماكرو هي إلى حد ما أقل ضررا من الأنواع الأخرى. عادة ما ينتشرون عبر البريد الإلكتروني. وهي من أكثر الفيروسات انتشارا وكما أنها تكتب بالورد او **Notepad**.

<u>مثال:</u> **<u>Melissa</u>**: فيروس ماكرو شهير يصيب ملفات الـ **Word** في **Microsoft Office 97** و **2000** ظهر أول مرة في ربيع عام 1999. يصل إلى المستخدم كرسالة بريد إلكتروني مع ملف مرفق يكون عنوان الرسالة **An Important Message From <<u>user</u>>** حيث يكون **<u>user</u>** هو أحد الأشخاص من دفتر العناوين لديك. عند فتح الملف المرفق يقوم الفيروس مباشرة إذا كان ***Microsoft Outlook*** منصباً بإرسال نفسه إلى أول 50 عنوان من دفتر العناوين لديك؛ ويقوم الفيروس بالتلاعب بسجلات النظام **System Registry**، يصيب الملف **Normal.dot** وهو قالب ملف الـ **Word** لأي ملف جديد، وبالتالي يضمن الفيروس إصابة أي ملف **Word** جديد به. ربما لا يمتلك **Melissa** آثاراً تدميرية كبيرة على الجهاز المصاب ولكنه يرهق حساب البريد الإلكتروني الخاص بك عبر زيادة عدد الرسائل المرسلة إليك مثلاً. تم تسمية هذا الفيروس بهذا الاسم بعد معرفة الشخص الذي صممه.

How Do They Infect

- **الفيروسات المخفية (Stealth Virus):**

هذه الفيروسات تحاول إخفاء نفسها عن برامج مكافحة الفيروسات. بمجرد إخفائها، فإنها تقوم بنسخ المعلومات من البيانات الغير مصابه على نفسها ثم تقوم بتصدير هذه البيانات إلى برنامج مكافحة الفيروسات أثناء الفحص. وهذا يجعل من الصعب الكشف او حذف هذا النوع من الفيروسات. يمكنه أن يصيب نظام الكمبيوتر بعدد من الطرق: على سبيل المثال، عندما يقوم المستخدم بتحميل مرفق البريد الإلكتروني الخبيثة؛ تثبيت البرمجيات الخبيثة المتنكرة في البرامج الحقيقية من المواقع؛ أو استخدام برامج لم يتم التحقق منها. مثل الفيروسات الأخرى، حيث يمكنها أن يستخدم طائفة واسعة من مهام النظام والتي يمكن أن تؤثر على أداء الكمبيوتر. عند تنفيذ مثل هذه المهام، فان برامج مكافحة الفيروسات تكتشف البرامج الضارة هذه، ولكن تم تصميم هذا الفيروس لكي يجعل نشاطه مخفي عن برامج مكافحة الفيروسات. فإنه يحقق هذا عن طريق تحريك نفسها مؤقتا بعيدا عن الملف المصاب ونسخ نفسها إلى محرك أقراص آخر واستبدال نفسها مع ملف نظيفة. يمكن للفيروس الشبح أيضا تجنب الكشف عن طريق إخفاء حجم الملف الذي أصيب.

يمكنك الكشف عن الفيروس قبل بدء تشغيل النظام عبر قرص تمهيد -لتجنب التحكم في النظام من قبل الفيروس -ومن ثم تبدأ في فحص الفيروسات. ومع ذلك، حتى لو كان الكشف عن هنا، فهناك فرصة أن الفيروس قد ينسخ نفسه إلى ملف آخر على النظام، لذلك لا يزال هذا الفيروس تحديا للقضاء عليه بشكل كامل.

- **فيروسات النفق (Tunneling Viruses):**

Tunneling virus هو الفيروس الذي يحاول التصدي للبرمجيات المكافحة ضد الفيروسات قبل أن تتمكن من الكشف عن الأكواد الخبيثة. هذا النوع من الفيروسات تقوم بتشغيل نفسها في مستوى أدني من إطار برامج مكافحة الفيروسات. حيث ثم تعمل من خلال الذهاب الى

interruption handlers في نظام التشغيل وإيقافها، وبالتالي تتجنب الكشف. برامج اعتراض، التي لا تزال تعمل في خلفية نظام التشغيل أصبحت خامله أثناء عمل **Tunneling virus**. بعض برامج مكافحة الفيروسات لا تجد الأكواد الخبيثة المرفقة لفيروسات النفق. لمكافحة هذه، فان بعض برامج مكافحة الفيروسات تستخدم أساليبهم الخاصة **tunneling**، والتي تكشف عن الفيروسات الخفية التي تقع داخل ذكريات الكمبيوتر.

Tunneling virus تحاول تجاوز مراقبة النشاط من قبل برامج مكافحة الفيروسات باتباع سلسلة المقاطعة وذلك بالرجوع إلى **DOS or BIOS interrupt handler's** ثم تثبيت نفسها.

- **فيروس التشفير (Encryption Viruses):**

هذا النوع من الفيروس يتكون من نسخة مشفرة من الفيروس ووحدة فك التشفير. لا تزال وحدة فك التشفير ثابتة، في حين يتم استخدام مفاتيح مختلفة للتشفير.

- **فيروسات متعددة الاشكال (Polymorphic Viruses):**

لقد تم تطوير هذه الفيروسات للتشويش على برامج مكافحة الفيروسات التي تفحص بحثا عن الفيروسات في النظام. فمن الصعب تتبعهم، نظرا لأنهم يغيرون خصائصها في كل مرة يصيبون النظام، على سبيل المثال، كل نسخة من هذا الفيروس تختلف عن السابقة. ومطوري الفيروسات قاموا بإنشاء المحركات المتحولة والمستلزمات لكتابة الفيروسات (***virus writing tool kits***) والتي تجعل اكواد هذا الفيروس الحالية تبدو مختلفة عن الآخرين من نوعها.

- **الفيروسات المتحولة (Metamorphic Viruses):**

الأكواد التي يمكن إعادة برمجة نفسها يطلق عليها **metamorphic code**. حيث يترجم هذا الكود إلى كود مؤقت، ومن ثم تحويلها إلى الكود العادي. هذه التقنية، التي لا تزال فيها الخوارزمية الأصلية سليمة، ويستخدم لتجنب التعرف على نمطها من قبل برامج مكافحة الفيروسات. هذه الفيروسات أكثر فعالية بالمقارنة مع **polymorphic code**. هذا النوع من الفيروسات تتكون من اكواد معقدة.

- **فيروس التجويف (Overwriting File or Cavity Viruses):**

بعض ملفات البرامج لديها مناطق من المساحات الفارغة. هذا الفضاء الفارغ هو الهدف الرئيسي لهذه الفيروسات. فيروس التجويف، والمعروف أيضا باسم **Space Filler Virus**، يخزن الأكواد الخاصة به في هذا الفضاء الفارغ. الفيروس يقوم بتثبيت نفسه في هذا الفضاء الغير مأهول دون أي تدمير للكود الأصلي للبرنامج. لأنه يثبت نفسه في ملف يحاول ان يصيبه.

- **Sparse Infector Viruses:**

Sparse infector virus هو نوع من الفيروسات لا يعمل إلا عند شرط معين ويبقى الـ **sparse infector** مخفياً داخل النظام ولا يشعر به المستخدم إلا عند شرط محدد بشكل رقمي كتاريخ معين أو كتشغيل برنامج ما عددٍ من المرات.

- **الفيروس المرافق (Companion Viruses):**

Companion virus هو فيروس كمبيوتر معقد، وهو على عكس الفيروسات التقليدية، لا تقوم بالتعديل على أي من الملفات. بدلا من ذلك، تقوم إنشاء نسخة من الملف وتضع ملحق آخر على ذلك، عادة (**.com**)(**مثلا file.exe الى file.com**) وبمجرد تنفيذ هذا الملف، فان الفيروس يصيب جهاز الكمبيوتر. هذه النوعية فريد بحيث يجعل الفيروس رفيق يصعب اكتشافه، كما يميل البرمجيات المضادة للفيروسات لاستخدام التغييرات في الملفات كدليل على وجود الفيروس. هذه الفيروسات من النوع القديم من الفيروس الذي كان أكثر وضوحا في عهد **MS-DOS**. يتم نشر ذلك في الغالب من خلال التدخل البشري.

- **فيروسات التمويه (Camouflage Viruses):**

هذه الفيروسات تخفي نفسها على أنها تطبيقات حقيقية للمستخدم. هذه الفيروسات ليس من الصعب العثور منذ أن تقدمت برامج مكافحة الفيروسات إلى النقطة التي يتم فيها تتبع مثل هذه الفيروسات بسهولة.

- **فيروسات القذيفة (shell viruses):**

اكواد هذه الفيروسات تشكل طبقة حول اكواد البرنامج المضيف الهدف التي يمكن مقارنتها مثل "قشرة البيضة"، مما يجعل من نفسه البرنامج الأصلي وأكواد المضيف تعتبر روتين فرعى. هنا، يتم نقل التعليمات البرمجية الأصلية إلى موقع جديد بواسطة اكواد الفيروس والفيروس هو الذي يقوم بتعريفها.

- **فيروسات امتداد الملفات (File Extension Viruses):**

File extension viruses تقوم بتغير امتدادات الملفات; حيث ان **.TXT** بيكون امن وهذا يشير الى ملف نصى نقى. فاذا تم غلق امكانيه رؤية امتدادات الملفات ثم قام شخص ما بارسال الملف **BAD.TXT.VBS** فإنك سوف ترى فقط **BAD.TXT**.

- **Add-on Viruses:**

معظم الفيروسات هي **add-on viruses**. هذا النوع من الفيروسات يلحق الأكواد الخاصة به إلى بداية اكواد المضيف بدون إجراء أية تغييرات عليه.

وبالتالي، فإن الفيروس يفسد معلومات بدء التشغيل لاكواد المضيف، ويضع نفسه في مكانها، ولكنها لا تلمس اكواد المضيف. ومع ذلك، يتم تنفيذ اكواد الفيروس قبل اكواد المضيف. الاشارة الوحيد على أن الملف تالف أي مصاب بهذا النوع من الفيروس هو أن حجم الملف قد ازداد.

- **الفيروسات المتطفلة (Intrusive Viruses):**

هذا النوع من الفيروس يقوم بكتابة اكواده فوق اكواد التطبيقات إما عن طريق الإزالة التامة لاكواد البرنامج المضيف الهدف، أو في بعض الأحيان فإنه الكتابة تكون فوق جزء منه فقط. لذلك، لا يتم تنفيذ التعليمات البرمجية الأصلية بشكل صحيح.

- **فيروسات العمل المباشر أو العابرة (Direct Action or Transient Viruses):**

هذه الفيروسات تقوم بنقل جميع الضوابط إلى اكواد المضيف حيث يقيم، ويختار البرنامج الهدف المراد تعديله، ويفسد عليه.

- **Tenninate and Stay Resident Viruses (TSRS):**

فيروس **TSR** يبقى بشكل دائم في الذاكرة أثناء دورة العمل بأكملها، حتى بعد تنفيذ البرنامج المضيف الهدف وإنهاؤها. لا يمكن إزالته إلا عن طريق إعادة تشغيل النظام.

فيروسات قطاع التشغيل (System/Boot Sector Virus)

System sector virus يمكن تعريفه بأنها تلك التي تؤثر على الأكواد القابلة للتنفيذ (*executable code*) من القرص، أما بالنسبة لـ **Boot sector virus** فيمكن تعريفه على انها تلك التي تؤثر على **DOS boot sector** من القرص الصلب.

قبل أن تتمكن من فهم ما يقوم به **Boot sector virus**، فمن المهم أن نعرف ما هو قطاع التمهيد(*boot sector*) . ويتكون القرص الصلب من العديد من **segment** ومجموعات من **cluster** من **segment**، والتي قد تكون مفصولة بشيء يسمى **partition**. يجب أن يكون هناك وسيلة للعثور على جميع البيانات المنتشرة في هذه **segment**، وهكذا فان عمل قطاع التمهيد (*boot sector*) كأنه **virtual Dewey Decimal system**. يحتوي كل قرص أيضا على (**MBR**) الذي يحدد موقع ويدير الأول من أي ملفات نظام التشغيل الضرورية اللازمة لتسهيل تشغيل القرص.
عندما يقرأ القرص، فانه يسعى أولا الى **MBR**، والذي من خلاله يمرر التحكم إلى قطاع التمهيد(*boot sector*) ، والتي توفر بدورها المعلومات ذات الصلة حول ما يقع على القرص وحيث يقع ذلك. يحتوي قطاع التمهيد (*boot sector*) أيضا المعلومات التي تحدد نوع وإصدار نظام التشغيل وتهيئة القرص مع.

ملخص هذا أن أي نظام ينقسم الى عدة مناطق تلك المناطق يطلق عليها سكتور (*sector*) أي القطاعات، حيث يتم تخزين التطبيقات/البرامج. وكما يشير اسمها، **system sector (or boot sector) viruses** تقوم بزرع نفسها في قطاعات (*sector*)نظام الكمبيوتر. قطاعات النظام هي مناطق خاصة على القرص، التي تحتوي على البرامج التي يتم تنفيذها، عند تشغيل جهاز الكمبيوتر الخاص بك. القطاعات ليست ملفات، ولكن ببساطة عباره عن مناطق صغيرة على القرص، أن الجهاز يقرأ قطاع واحد. هذه القطاعات هي غير مرئية للبرامج العادية ولكنها مهمه بالنسبة لعملية التشغيل الصحيحة لجهاز الكمبيوتر الخاص بك. والتي تعتبر هدف حيوي بالنسبة للفيروس.

هناك نوعان من قطاعات النظام التي توجد على أجهزة الكمبيوتر ويندوز/دوس:

DOS boot sectors and partition sectors (also known as master boot records or MBR)

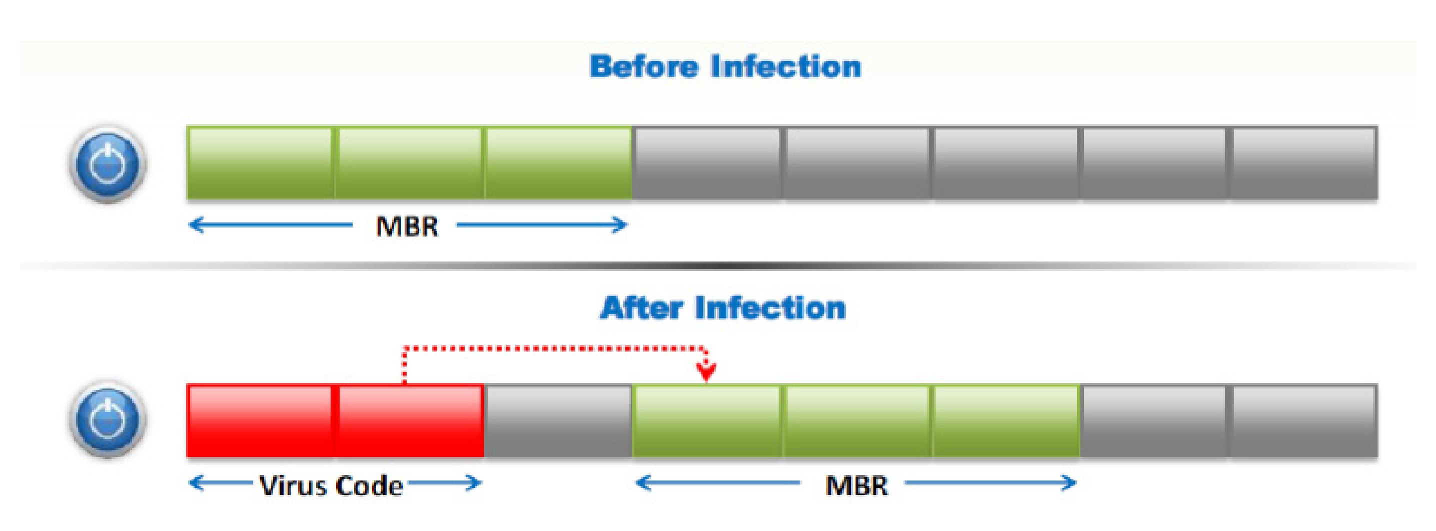
- **MBR (Master Boot Record)**

MBRs هي أكثر المناطق المعرضة للفيروسات لأنه إذا حدث تلف لـ **MBR**، فانه سيتم فقدان جميع البيانات. هذا الجزء في الأنظمة الحديثة التي تعتمد على **BIOS** من النوع **UEFI** قد تم استبداله الى نظام **GPT**.

- **DBR (DOS Boot Record)**

يتم تنفيذ القطاع **DBR** كلما يتم تشغيل النظام. حيث تعتبر هذه هي النقطة الحاسمة للهجوم من قبل الفيروسات.

قطاع النظام (*System sector*) يتكون من 512 بايت من الذاكرة. وبما انه ليس هناك الكثير من المساحات في قطاع النظام، فان هذه الفيروسات غالبا ما تقوم بإخفاء التعليمات البرمجية الخاصة بها في مكان آخر على القرص. والتي في بعض الأحيان يسبب مشاكل عند هذه البقعة التي تحتوي بالفعل على البيانات، إذا حدث إعادة الكتابة عليها. ولكن في بعض الأحيان فان **Boot sector virus** يقوم بتحريك **MBR** إلى موقع آخر على القرص الثابت ونسخ نفسه إلى الموقع الأصلي من **MBR**. فعندما يبدا تشغيل نظام التشغيل فانه يبدا أولا بتشغيل الأكواد الخاصة بالفيروس ومن ثم ينقل التحكم الى **MBR**.



الحامل الرئيسي لـ **System sector virus** هو **floppy disk**. هذه الفيروسات يقيمون عادة في الذاكرة. كما أنها يمكن أن تكون ناجمة عن حصان طروادة. أيضا بعض من **sector virus** تنتشر من خلال الملفات المصابة، ويطلق عليها أيضا فيروسات متعددة الأجزاء (***multipart viruses***).

إزالة الفيروس (Virus Removal)

تم تصميم نظام فيروسات القطاع (**sector virus**) لخلق الوهم بأنه ليس هناك أي فيروس على النظام. طريقة واحدة للتعامل مع هذا النوع من الفيروس هو تجنب استخدام نظام التشغيل ويندوز، والتحول إلى لينكس أو ماك، وذلك لأن ويندوز هو أكثر عرضة لهذه الهجمات. لينكس وماكنتوش يحتوي على **safeguard** مدمجة به وذلك للحماية ضد هذه الفيروسات. والطريقة الأخرى هي تنفيذ الفحص من قبل تطبيقات مكافحة الفيروسات على أساس دوري وهذا صعب جدا في اكتشافه.

File and Multipartite Viruses

فيروسات الملفات (File viruses)

فيروسات الملفات تصيب الملفات التي يتم تنفيذها أو تفسيرها من قبل النظام مثل **COM**، **EXE**، **SYS**، **OVL**، **OBJ**، **PRG**، **MNU**، وملفات **BAT**. فيروسات الملفات يمكنها أن تكون إما تعمل مباشرة (**direct-action (non-resident)**) أو تقيم في الذاكرة **memory-resident**. مطورو هذه الفيروسات يسببوا ضررا لا رجعة فيه إلى الملفات. هذه الفيروسات تستهدف أساسا مجموعة من أنظمة التشغيل التي تشمل ويندوز، يونيكس، دوس، وماكنتوش.



مميزات فيروسات الملف:

فيروسات الملف يتم تميزها ووصفها على أساس سلوكهم المادي (***Physical behavior***) أو الخصائص. يتم تصنيف فيروسات الملف على حسب نوع الملف الذي يستهدفه، مثل **EXE** أو ملفات**COM** ، قطاع التمهيد وما الى ذلك. يمكن أيضا أن يتم وصف فيروس ملف على اساس كيفية إصابته الملف المستهدف (المعروف أيضا باسم ملفات المضيف):

Prepending: يكتب نفسه في بداية اكواد الملف المضيف.

Appending: يكتب نفسها إلى نهاية الملف المضيف

Overwriting: يقوم بالكتابة فوق اكواد الملف المضيف مع الأكواد الخاصة به.

Inserting: يقوم بإدراج نفسه في فجوات داخل كود الملف المضيف.
Companion: يقوم بإعادة تسمية الملف الأصلي ويكتب نفسه مع اسم الملف المضيف.
Cavity infector: يكتب نفسه بين أجزاء ملف ذات 32 بت.

تصنف فيروسات الملف أيضا على أساس ما إذا كانت غير مقيمه في الذاكرة أو مقيمة في الذاكرة. الفيروسات الغير مقيمه في الذاكرة تبحث عن ملفات **EXE** على القرص الصلب ثم تنقل العدوى اليه، في حين أن الفيروسات المقيمة في الذاكرة تبقى بنشاط في الذاكرة، وتصيد واحد أو أكثر من وظائف النظام. ويقال إن فيروسات الملف تكون متعددة الأشكال(***polymorphic***) ، مشفرة(***encrypted***)، أو غير مشفرة. الفيروسات متعدد الأشكال أو المشفر يحتوي على واحد أو أكثر من **decryptor** (فاكك التشفير) بالإضافة الى اكواده الرئيسية. يتم فك تشفير اكواد الفيروس الرئيسي بواسطة **decryptor** قبل أن تبدأ. يستخدم الفيروس المشفرة عادة **decryptor** متغير أو مفتاح ثابتة، في حين أن الفيروسات متعددة الأشكال تحتوي على **decryptors** يتم إنشاؤها عشوائيا من تعليمات المعالجات والتي تتكون من الكثير من الأوامر التي لا يتم استخدامها في عملية فك التشفير.

Execution of Payload (طرق تنفيذ الفيروس):

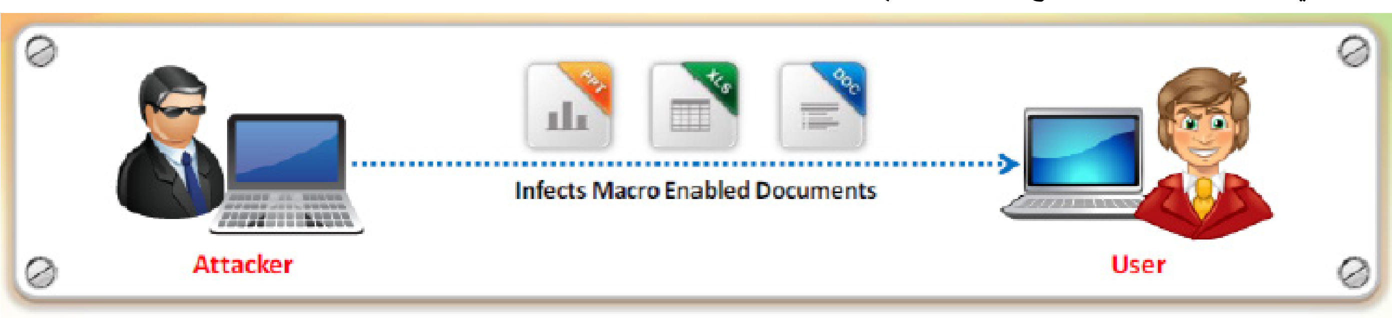
- Direct action: أي يتم تنفيذها فورا/مباشرة.
- Time bomb: يتم تنفيذها بعد فتره محدده من الوقت.
- Condition triggered: يتم تنفيذها تحت ظروف معينه.

Multipartite Viruses

Multipartite virus (فيروسات متعددة الأجزاء) يطلق عليه أيضا **multi-part virus** الذي تحاول مهاجمة كل من قطاع التمهيد والملفات القابلة للتنفيذ أو ملفات البرنامج في نفس الوقت. عندما يتم إرفاق الفيروس **RGW** إلى قطاع التمهيد، فانه سوف يؤثر بدوره على ملفات النظام، ومن ثم يرتبط الفيروس بالملفات، وهذه المرة سيقوم بدوره بإصابة قطاع التمهيد.

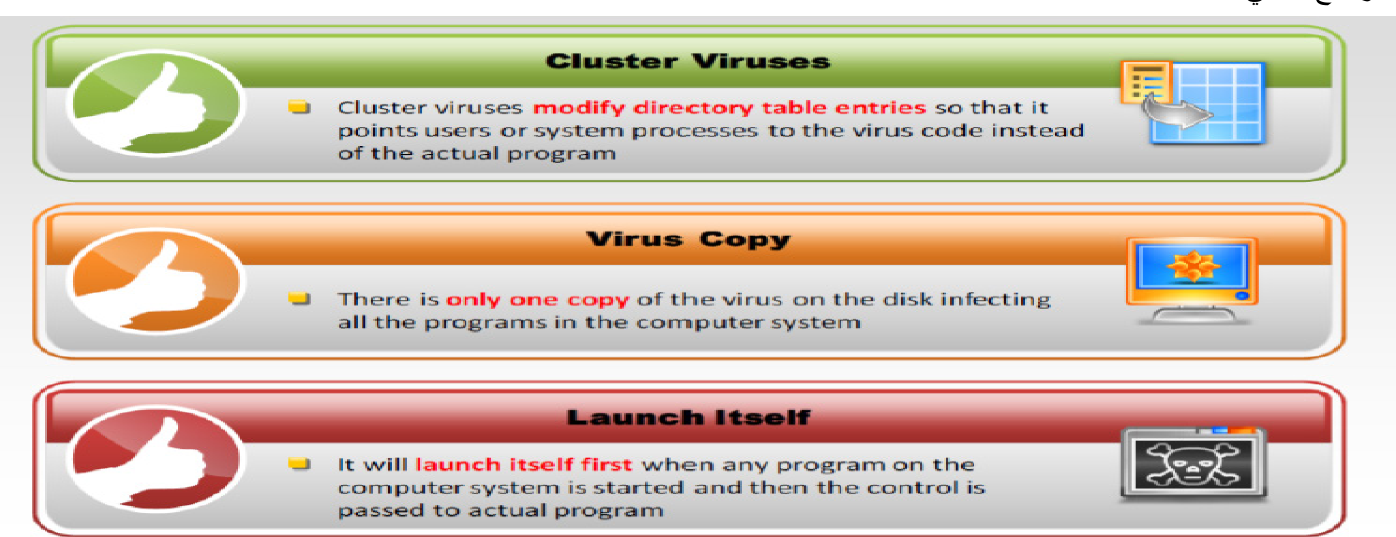
فيروسات الماكرو (Macro Viruses)

Microsoft Word أو التطبيقات المماثلة يمكنها أن تصاب بواسطة فيروسات الكمبيوتر ويسمى هدا النوع من الفيروسات فيروس الماكرو، والذي يؤدي تلقائيا سلسلة من الإجراءات عندما يتم تشغيل التطبيق أو أي شيء آخر. تتم كتابة معظم فيروسات الماكرو باستخدام لغة ماكرو **Visual Basic for Applications (VBA)** حيث أنها تصيب القوالب(***templet***) أو تقوم بتحويل الوثائق(***document***) المصابة إلى ملفات القالب (***templet file***)، مع الحفاظ على مظهرها على انها ملفات مستندات عادية. فيروسات الماكرو في كثير من الأحيان هو أقل ضررا من الأنواع الأخرى. عادة ما ينتشرون عبر البريد الإلكتروني. ملفات البيانات النقية لا تسمح بانتشار الفيروسات، ولكن أحيانا الخط الفاصل بين ملف البيانات والملف تنفيذي يتم التغاضي عنه بسهولة من قبل المستخدم العادي نظرا لاستخدام لغات الماكرو الواسعة في بعض البرامج. في معظم الحالات، فقط لجعل الامور سهلة بالنسبة للمستخدمين، فان الخط الفاصل بين ملف البيانات والبرامج تبدأ للتمويه فقط في الحالات التي يتم تعيين وحدات الماكرو الافتراضية للتشغيل تلقائيا في كل مرة يتم تحميل ملف البيانات. كاتبوا الفيروسات يمكنهم **exploit** برامج شائعة مع قدرة الماكرو مثل **Microsoft Word** و**Excel** وبرامج **Office** الأخرى. يمكن أيضا أن تحتوي ملفات المساعدة للويندوز (***Windows Help files***) على اكواد الماكرو. بالإضافة إلى ذلك، فان أحدث **exploit** لـ **macrocode** موجود في النسخة الكاملة من برنامج أكروبات الذي يقرأ ويكتب ملفات **PDF**.



الفيروسات العنقودية (Cluster Viruses)

Cluster virus's تصيب الملفات دون تغيير الملف أو زرع ملفات إضافية ولكن تقوم بتغير معلومات الدليل **DOS** بحيث تشير الادخالات إلى اكواد الفيروس بدلا من اكواد البرنامج الفعلي. عند تشغيل برنامج **DOS**، فانه يقوم أولا بتحميل وتشغيل اكواد الفيروس، ومن ثم يقوم الفيروس بتحديد موقع البرنامج الفعلي ويقوم بتشغيله. **DIR-2** هو مثال لهذا النوع من الفيروس. الفيروسات العنقودية تقوم بتعديل إدخالات جدول الدليل بحيث تشير إدخالات الدليل إلى اكواد الفيروس. هناك نسخة واحدة فقط من الفيروس على القرص تقوم بإصابة جميع البرامج في نظام الكمبيوتر. انها ستطلق نفسها أولا عند بدء أي من البرامج على نظام الكمبيوتر بالعمل ومن ثم يتم تمرير التحكم إلى البرنامج الفعلي.



Stealth/Tunneling Viruses

- **الفيروس الشبح (Stealth viruses)**

هذه الفيروسات تحاول إخفاء أنفسها من برامج مكافحة الفيروسات عن طريق تغيير النشاط وإفساد **service call interrupts** المختارة عندما يتم تشغيلها. حيث يتم استبدال طلبات تنفيذ العمليات التي تتعلق ب **service call interrupts** بأكواد الفيروس. هذه الفيروسات تعرض معلومات كاذبة لإخفاء وجودها عن برامج مكافحة الفيروسات. على سبيل المثال، حيث يقوم الفيروس الشبح بإخفاء العمليات التي تم تعديلها وإعطاء بدلا منها تمثيل زائفة. وبالتالي، فإنه يأخذ أجزاء من النظام الهدف ويخفي اكواد الفيروس فيها.

الفيروس الشبح يخفي نفسه عن برامج مكافحة الفيروسات عن طريق إخفاء الحجم الأصلي للملف أو وضع نسخة من نفسها مؤقتا في بعض الأقراص الأخرى للنظام، وبالتالي يستبدل الملف المصاب مع الملف السليم التي تم تخزينه على القرص الصلب.

الفيروس الشبح يقوم بإخفاء التعديلات التي يجريها. فإنه يأخذ السيطرة على وظائف النظام التي تقوم بقراءة الملفات أو قطاعات النظام، وعندما يطلب برنامج آخر المعلومات التي سبق تعديلها من قبل الفيروس، فان الفيروس الشبح يعطى تقارير عن تلك المعلومات إلى البرنامج الطالب بدلا من البرنامج الأصلي. يتواجد هذا الفيروس أيضا في الذاكرة.

لتجنب الكشف، هذه الفيروسات تأخذ دائما التحكم في وظائف النظام واستخدامها لإخفاء وجودها.

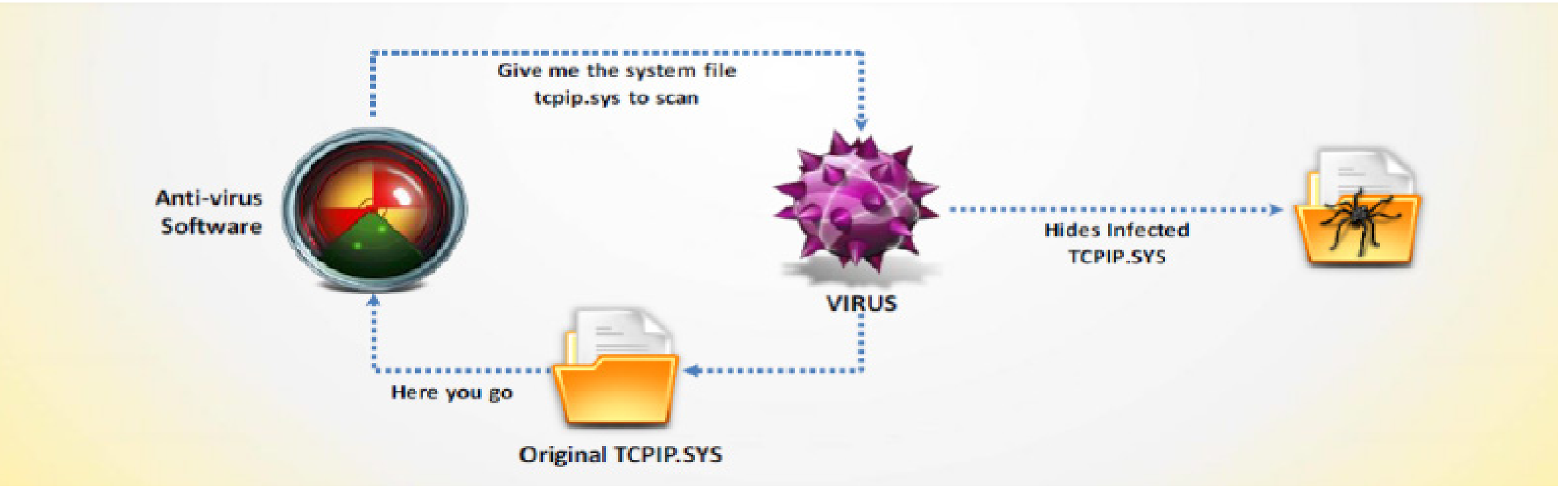
واحد من حوامل الفيروس الشبح هو **rootkit**. تثبيت **rootkit** عامة ينتج عنه هجوم هذا الفيروس وذلك لان **rootkit** يتم تثبيته من خلال حصان طروادة، وهذا قادر على إخفاء أي من البرمجيات الخبيثة.

إزالة الفيروس (virus removal)

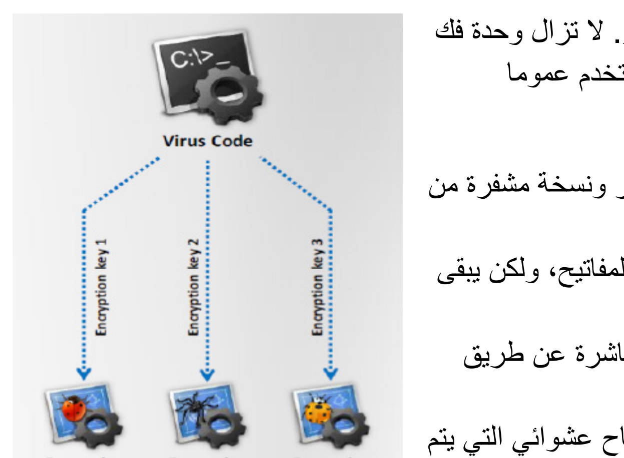
- دائما تفعيل التمهيد البارد{*cold boot*} (أي التمهيد من قرص مرن أو CD محمي ضد الكتابة)
- بدا استخدام أوامر **DOS** مثل **FDISK** لإصلاح الفيروس.
- استخدام برامج الحماية من الفيروسات.

- فيروس النفق (Tunneling viruses)

هذه الفيروسات تتبع خطوات برامج الاعتراض (*Interceptor programs*) التي ترصد طلبات نظام التشغيل لذلك فهيا تصل الى **BIOS** و**DOS** لتثبيت نفسها. لتنفيذ هذا النشاط، فأنها تنشأ نفق تحت برامج مكافحة الفيروسات.



الفيروس المشفر (Encryption Viruses)



هذا النوع من الفيروس يتكون من نسخة مشفرة من الفيروس ووحدة فك التشفير. لا تزال وحدة فك تشفير ثابتة، في حين أنه يتم استخدام مفاتيح مختلفة للتشفير. هذه الفيروسات تستخدم عموما **XOR** على كل بايت مع مفتاح عشوائي.

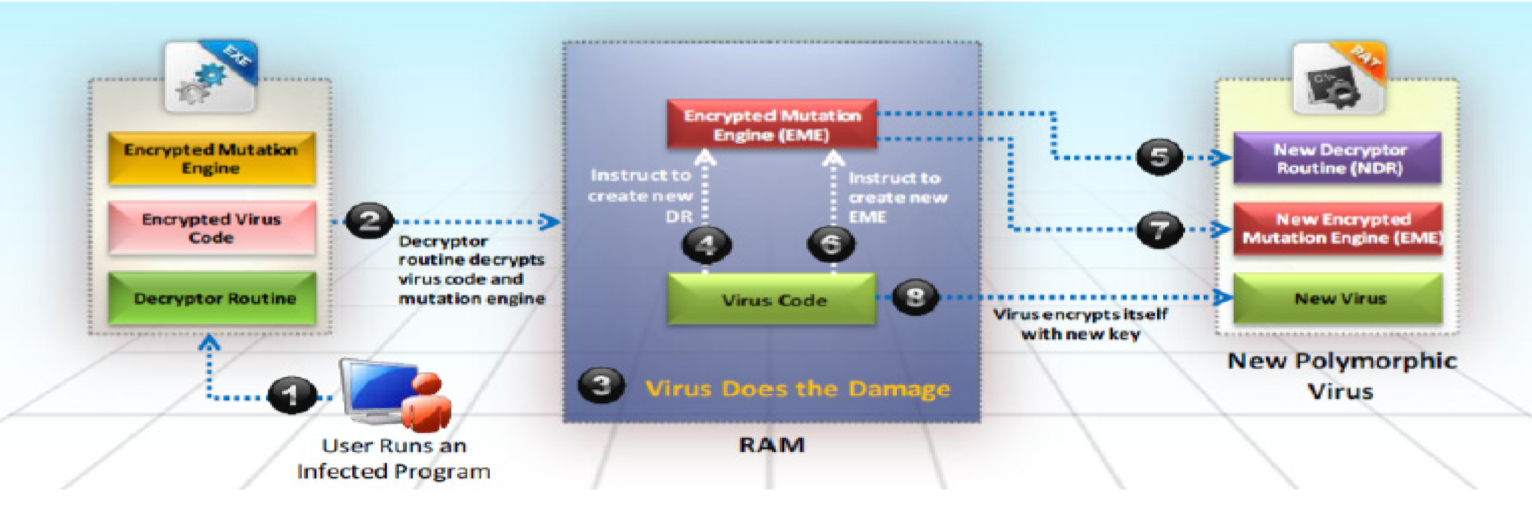
- يتم تشفير الفيروس مع مفتاح تشفير والذي يتكون من وحدة فك التشفير ونسخة مشفرة من التعليمات البرمجية.
- لكل ملف مصاب، يتم تشفير الفيروس باستخدام مجموعة مختلفة من المفاتيح، ولكن يبقى جزء وحدة فك التشفير دون تغيير.
- أنه من المستحيل لتطبيقات فحص الفيروسات الكشف عن الفيروس مباشرة عن طريق التوقيعات، ولكن يمكن أن يتم الكشف عن وحدة فك التشفير.
- تقنية التشفير المستخدمة هي عباره عن تضمين x أو كل بايت مع مفتاح عشوائي التي يتم إنشاؤها وحفظها بواسطة **virus root**.

فيروس متعدد الاشكال (Polymorphic Viruses)

الفيروسات متعددة الأشكال تقوم بتعديل الأكواد الخاصة بها لكل نسخه متماثله من أجل تجنب الكشف. أنها تنجز هذا عن طريق تغيير وحدة التشفير وتسلسل التعليمات. يتم استخدام مولد رقم عشوائي لتنفيذ تعدد الأشكال.

عموما يستخدم محرك الطفرة (*mutation engine*) لتمكين اكواد متعدد الأشكال. **Mutator** يوفر سلسلة من التعليمات التي يمكن استخدامها من قبل فاحص الفيروسات لتحسين خوارزمية الكشف المناسبة. وتستخدم اكواد متعددة الأشكال البطيئة لمنع مكافحي الفيروسات المحترفين من الوصول إلى الأكواد.

عينات الفيروس(*virus sample*) ، هي ملفات طعم (تستخدم لاصطياد اكواد الفيروس) بعد إصابة ملف تنفيذي واحد واحدة، وتحتوي على نسخة مماثلة للفيروس. ويستخدم فاحص سلامة بسيط (*simple integrity checker*) للكشف عن وجود الفيروس متعدد الأشكال في قرص النظام.



الفيروسات متعددة الأشكال (*Polymorphic viruses*) تتكون من ثلاثة عناصر. وهي اكواد الفيروس المشفر، روتين فك التشفير، ومحرك الطفرة(*mutant engine*) . وظيفة روتين فك التشفير(*decryptor routine*) هو فك شفرة الفيروس. حيث أنه يفك الشفرة فقط بعد السيطرة على جهاز الكمبيوتر. محرك الطفرة (*mutant engine*) يولد روتين فك التشفير (*decryptor routine*) عشوائيا. روتين فك التشفير (*decryptor routine*) يختلف في كل مرة عندما يتم إصابة برنامج جديد بواسطة الفيروس.

مع فيروس متعدد الأشكال، يتم تشفير كل من محرك الطفرة وأكواد الفيروس. عندما يتم تشغيل برنامج مصاب بالفيروس متعددة الأشكال من قبل المستخدم، فان روتين فك التشفير(*decryptor routine*) يأخذ السيطرة الكاملة على النظام، وبعد ذلك يفك شفرة الفيروس ومحرك الطفرة. ثم بعد ذلك، يتم نقل السيطرة على النظام الخاص بك عن طريق روتين فك التشفير(*decryptor routine*) الى الفيروس، والذي يذهب الى برنامج جديد لنقل العدوى. في ذاكرة الوصول العشوائي (**RAM**)، يقوم الفيروس بنسخ نسخة طبق الأصل منه وكذلك محرك الطفرة. ثم بعد ذلك يرشد الفيروس محرك الطفرة المشفر لتوليد روتين فك التشفير الجديد عشوائيا، التي لديها القدرة على فك تشفير الفيروس. هنا، يتم تشفير نسخة جديدة من كل من اكواد الفيروس ومحرك الطفرة من الفيروس. وبالتالي، فإن هذا الفيروس، يكون بجانب اكواد الفيروس التي تم تشفيرها حديثا وكذلك محرك الطفرة(**EME**) المشفر الجديد، ثم يلحق روتين فك التشفير الجديد هذا على برنامج جديد، وبالتالي تستمر هذه العملية.

الفيروسات متعددة الأشكال التي أعدت من قبل المهاجم لتنتشر في النظم المستهدفة يصعب كشفها لأنه هنا يتم تشفير جسم الفيروسات وإجراءات فك التشفير يتغير في كل مرة من الإصابة للإصابة وإصابة شخصين لا تبدو هي نفسها؛ هذا يجعل من الصعب على مكافح الفيروسات تحديد هذا الفيروس.

الفيروسات المتحولة (Metamorphic Viruses):

بعض الفيروسات تعيد كتابة أنفسهم لتصيب ملفات تنفيذيه جديده. مثل هذه الفيروسات تكون معقدة وتستخدم المحركات المتحولة (*metamorphic engines*) للتنفيذ.

يطلق على الأكواد التي يمكن إعادة برمجة نفسه الأكواد المتحولة(*metamorphic code*) . ويترجم هذا الكود إلى كود مؤقت، ومن ثم تحويله مرة اخرى إلى كود العادي. هذه التقنية، تكون الخوارزمية الأصلية فيها لا تزال سليمة، حيث يستخدم هذا لتجنب التعرف على النمط من قبل برامج مكافحة الفيروسات. هذا أكثر فعالية في المقارنة بالاكواد متعددة الأشكال. هذا النوع من الفيروسات تتكون من مجموعه من الأكواد المعقدة.

الفيروسات المتحولة المعروفة هي:

Win32/Simile:

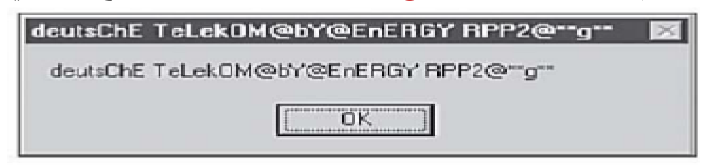
هذا الفيروس مكتوب بلغة التجميع (*assembly language*) حوالي 14000 سطر وتم تصميمه من أجل أنظمة التشغيل مايكروسوفت ويندوز. هذه العملية معقدة، ويتم إنشاء ما يقرب من 90٪ من اكواد الفيروس عن طريق هذه العملية (أي ان 90% من الفيروس عباره عن اكواد متحولة (*metamorphic codes*)).

:Zmist

هذا الفيروس معروف أيضا باسم **Z0mbie.Mistfall** التي أنشائها كاتب الفيروس الروسي المعروف باسم **Z0mbie**. وهو أول فيروس استخدم تقنية تسمى "**code integration**". هذا الكود يدرج نفسه في الأكواد الأخرى، يعيد إنشاء الأكواد، ثم يعيد بناء الملف القابل للتنفيذ.



a.) Variant A



c.) The "Unofficial" Variant C



b.) Variant B



d.) The .D variant (which was the "official" C of the original author)

File Overwriting or Cavity Viruses

هذه الفيروسات تعرف أيضا باسم **space-fillers** لأنها تحافظ على ثابت حجم الملف عندما يتم إصابته عن طريق تثبيت نفسه في البرنامج الهدف. هم يقومون بإلحاق أنفسهم إلى نهاية الملفات وأيضا إفساد بداية الملفات. هذا الحدث يقوم أولا بتنشيط وتنفيذ التعليمات البرمجية الخاصة بالفيروس، وبعدها البرنامج الأصلي.

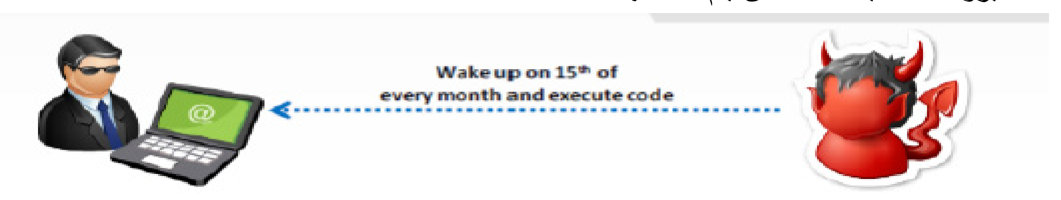
بعض ملفات البرامج لديها مناطق من المساحة الفارغة. هذا الفضاء الفارغ هو الهدف الرئيسي من هذه الفيروسات. فيروس التجويف، والمعروف أيضا باسم فيروس **space-fillers**، يخزن الأكواد الخاصة به في هذا الفضاء الفارغ. الفيروس يقوم بتثبيت نفسه في هذا الفضاء الغير مأهول دون أي تدمير للكود الأصلي. لأنه يثبت نفسه في ملف يحاول إصابته.

نادرا ما يستخدم هذا النوع من الفيروسات لأنه من الصعب أن يكتب. ملف ويندوز جديد يسمى **Portable Executable** إنها مصممة للتحميل السريع للبرامج. ومع ذلك، فإنه يترك فجوة معينة في الملف بينما يتم تنفيذه والتي يمكن استخدامها من قبل فيروسات **Space Filler** لإدراج نفسها. عائلة الفيروس الأكثر شعبية هي فيروس **CIH**.



Sparse Infector Viruses

Sparse infector virus's هو نوع من الفيروسات لا يعمل إلا عند شرط معين ويبقى الـ **sparse infector** مخفياً داخل النظام ولا يشعر به المستخدم إلا عند شرط محدد بشكل رقمي كتاريخ معين أو كتشغيل برنامج ما عددٍ من المرات. عن طريق الإصابة الأقل، في محاولة من قبل هذه الفيروسات لتقليل احتمال أن يتم اكتشافها.

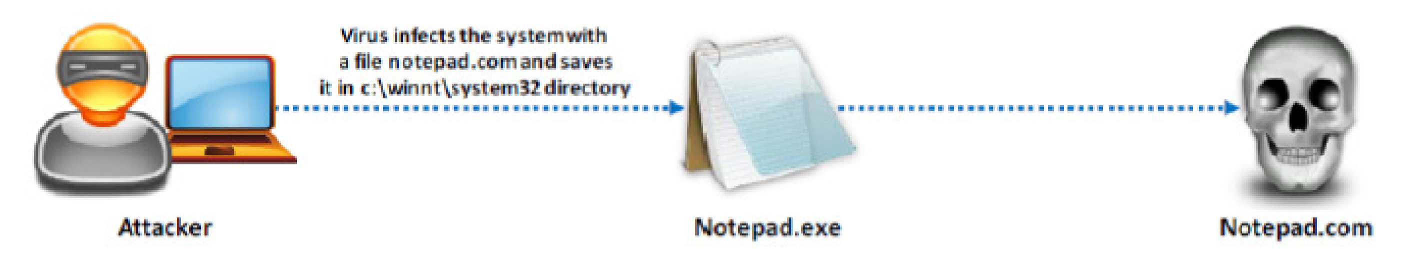


Companion/Camouflage Viruses

Companion virus يخزن نفسه من خلال امتلاك اسم الملف متطابقة كما في ملف البرنامج المستهدف. حالما يتم تنفيذ هذا الملف، فإن الفيروس يصيب جهاز الكمبيوتر، ويتم تعديل البيانات على القرص الصلب.

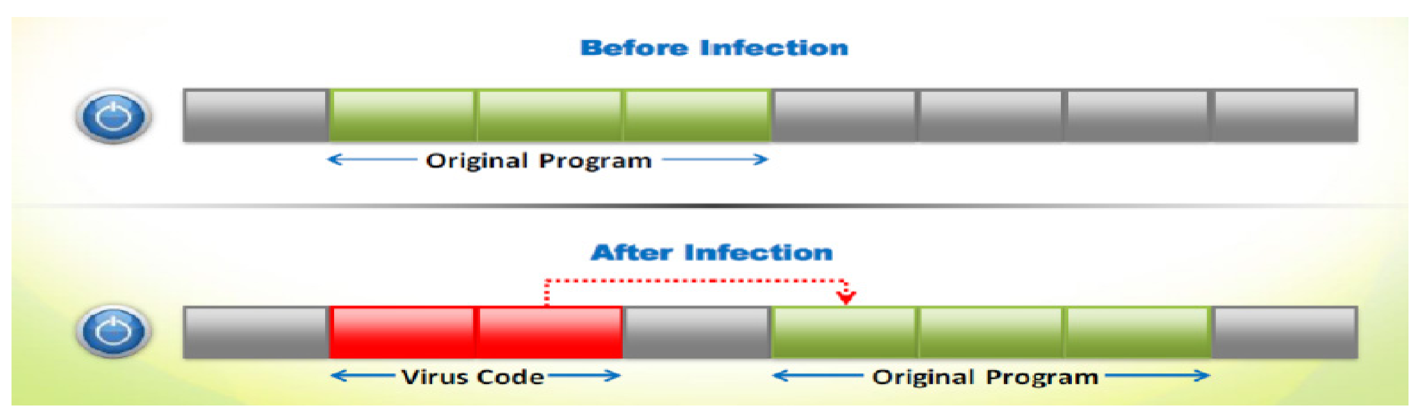
Companion virus يستخدم **DOS** التي تنفذ الملفات **COM** قبل أن يتم تنفيذ الملفات **EXE**. الفيروس يقوم بتثبيت ملف **COM** متطابقة ويصيب ملفات **EXE**.

المصدر: http://www.cknow.com/cms/vtutor/companion-files.html
هل تعتقد أن الفيروس يمكنه أن يصيب الملفات الخاصة بك دون تغيير بايت واحد في الملف المصاب؟ حسنا، هذا صحيح؛ بطريقتين مختلفتين في الواقع! وتسمى الطريقة الأكثر شيوعا من الطريقتين **companion virus** أو **spawning virus** (الآخر هو الفيروس العنقودي(***cluster virus***)). الفيروس يصيب ملفاتك عن طريق تحديد موقع كل الملفات التي تنتهي أسماؤها ب**EXE** . ثم يقوم الفيروس بإنشاء اسماء ملفات مطابقة تنتهي بـ **COM** الذي يحتوي على اكواد الفيروس.
هذا ما يحدث: دعونا نقول إن **companion virus** تنفذ على جهاز الكمبيوتر الخاص بك، وتقرر ان الوقت قد حان لتصيب الملفات. فإنه ينظر حوله ويبحث للعثور على ملف يسمى **PGM.EXE**. عليه الآن إنشاء ملف يسمى **PGM.COM** التي تحتوي على الفيروس. الفيروس عادة ما يزرع هذا الملف في نفس مسار ملف **EXE**. ولكن يجب وضعه في أي دليل على مسار **DOS** الخاص بك. حيث إذا قمت بكتابة **PGM** ثم نقرت فوق **Enter**، فان **DOS** سوف يقوم بتنفيذ **PGM.COM** بدلا من **PGM.EXE**. (حيث ان النظام المتبع من قبل **DOS**، انه يقوم أولا بتنفيذ **COM**، ثم **EXE**، ثم ملفات **BAT** الذي يحمل نفس الاسم الجذر، إذا كانت كلها في نفس الدليل). ينفذ الفيروس، وربما يصيب الكثير من الملفات ثم يقوم بتحميل وتنفيذ **PGM.EXE**. المستخدم ربما لن يلاحظ أي شيء خاطئ.
إنه من السهل الكشف عن الفيروس **companion virus** وذلك فقط من خلال ملاحظة وجود ملف **COM** إضافية على النظام.



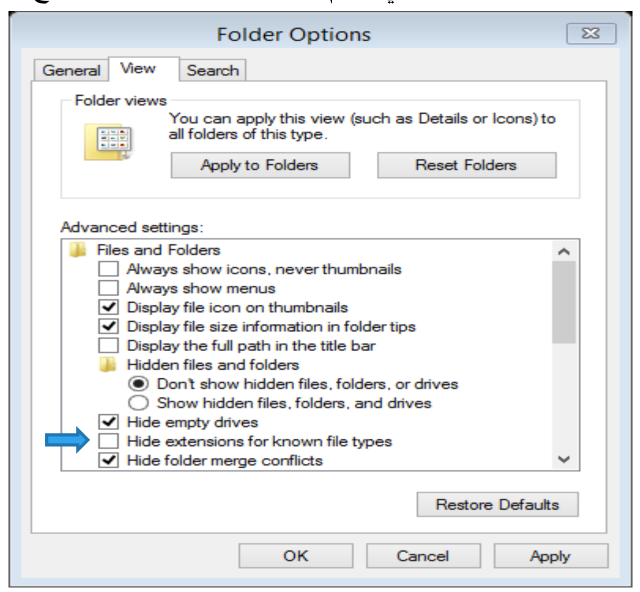
Shell Viruses

اكواد فيروس الشل (**shell virus**) تشكل طبقة حول كود البرنامج المضيف الهدف التي يمكن مقارنتها بـ "قشرة البيضة"، مما يجعل من نفسه البرنامج الأصلي وكود المضيف عباره عن امر فرعي. هنا، يتم نقل الأكواد الأصلية إلى موقع جديد بواسطة كود الفيروس والفيروس يقترض هويتها.



File Extension Viruses

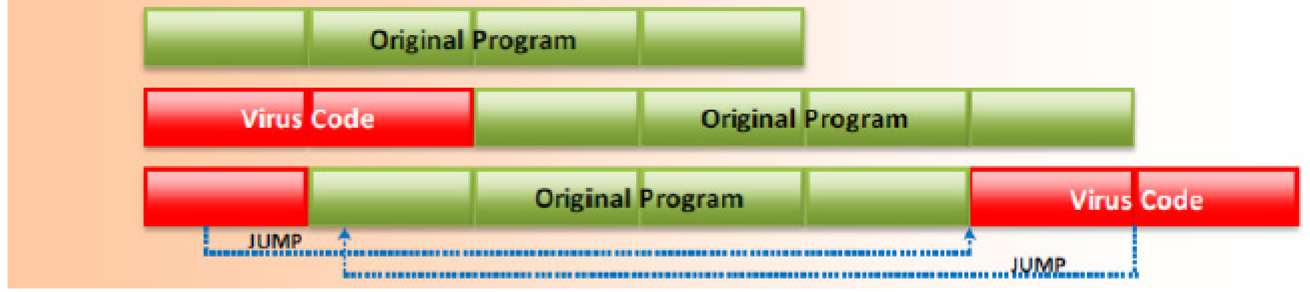
- **File extension virus** يغير امتدادات الملفات.
- (**.txt**) هو ملف امن لأنها تشير الى ملف نصي نقي.
- مع إيقاف تشغيل خاصية **File name extension**، فإذا قام شخص ما بارسال ملف لك اسمه **BAD.TXT.VBS**، فإنك سوف تراه **BAD.TXT** فقط.
- إذا كنت قد نسيت أن **File name extension** في قد تم إيقاف تشغيلها، فإنك سوف تعتقد ان هذا الملف ملف نصي وسوف تقوم بفتحه.
- **Visual Basic Script virus** هذا هو ملف الفيروس القابل للتنفيذ والذي يمكن القيام بأضرار جسيمة.
- التدابير المضادة هو إلغاء خاصية إخفاء الامتدادات في نظام التشغيل ويندوز. حيث تصبح كالاتى كما هو موضح في الصورة.



Add-on and Intrusive Viruses

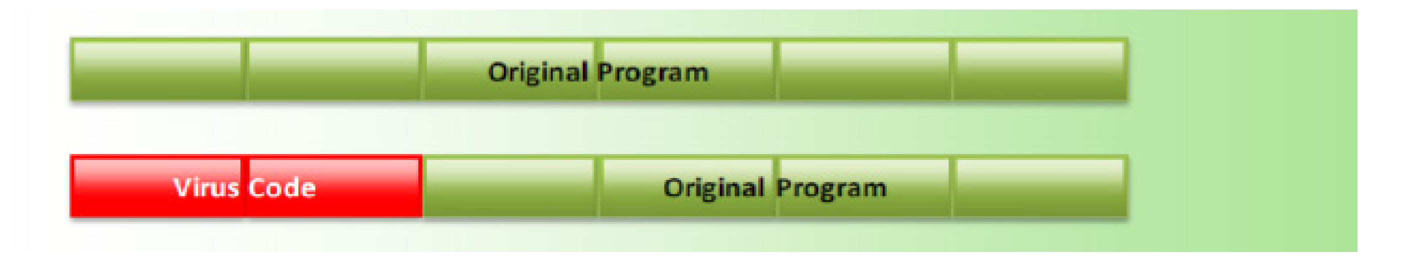
Add-on Viruses

معظم الفيروسات هي **Add-on Viruses**. هذا النوع من الفيروسات يُلحق الأكواد الخاصة به إلى بداية اكواد تطبيق المضيف دون إجراء أية تغييرات على هذه. وبالتالي، فإن الفيروس يفسد معلومات بدء التشغيل من اكواد المضيف، ويضع نفسه في مكانها، ولكنها لا تلمس اكواد المضيف. ومع ذلك، يتم تنفيذ اكواد الفيروس قبل اكواد المضيف. إشارة فقط الى أن الملف تالف هو أن حجم الملف قد ازداد.



Intrusive Viruses

الفيروسات المتطفلة (*Intrusive Viruses*) تقوم بإعادة كتابة الأكواد الخاصة بها إما عن طريق إزالة اكواد البرنامج المضيف الهدف تماما أو في بعض الأحيان تتم الكتابة سوى جزء منه. لذلك، لا يتم تنفيذ الأكواد الأصلية بشكل صحيح.



Transient and Terminate and Stay Resident Viruses

Transient Viruses

Transient virus تقوم بنقل جميع السيطرة إلى الأكواد المضيفة التي يقيمون فيها، حيث تحدد البرنامج الهدف لتعديله، وإفساده.

Terminate and Stay Resident Virus (TSR)

تبقى فيروسات **TSR** بشكل دائم في الذاكرة أثناء دورة العمل بأكملها، حتى بعد تنفيذ البرنامج المضيف الهدف وإنهاؤها. ولا يمكن إزالتها إلا عن طريق إعادة تشغيل النظام.

كتابة برنامج فيروس بسيط (Writing a Simple Virus Program)

لأغراض العرض التوضيحي، هنا يظهر برنامج بسيط والتي يمكن استخدامه للتسبب بالضرر للنظام المستهدف:

1- إنشاء ملف باتش **Game.bat** مع النص التالي:

text @ echo off
delete c:\winnt\system32*.*
delete c:\winnt*.*

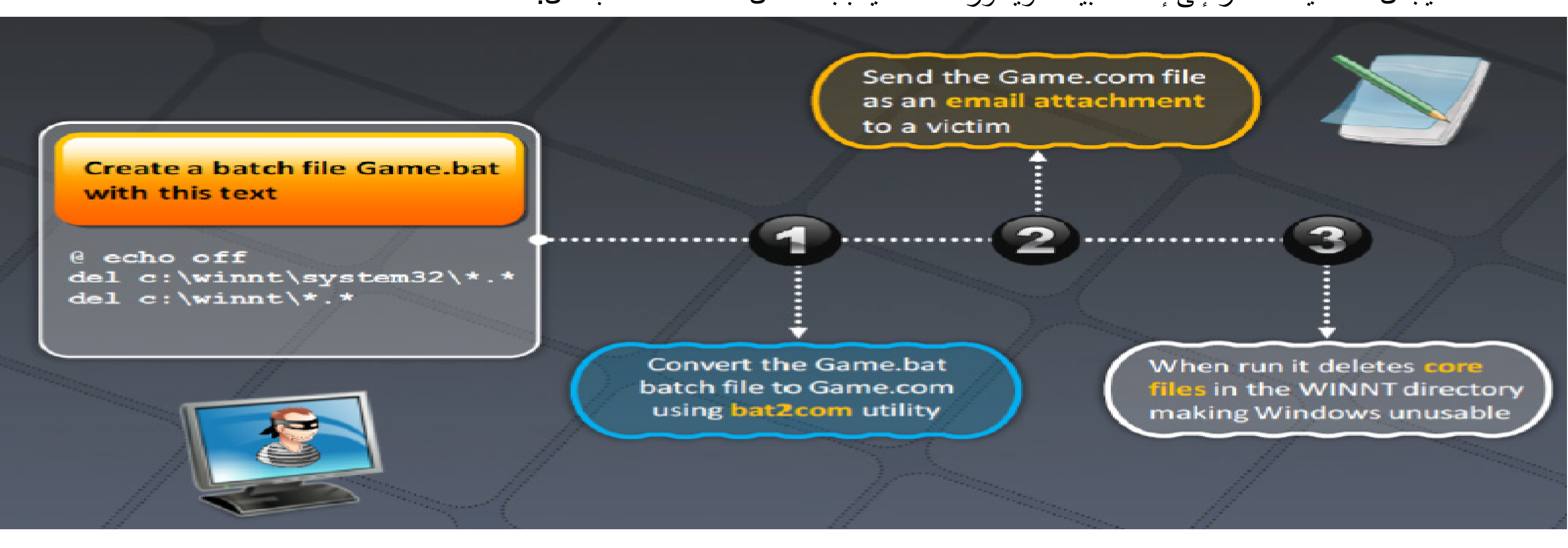
2- ثم قم بتحويل ملف الباتش **Game.bat** الى **Game.com** باستخدام الأداة المساعدة **bat2com**.

3- نقوم بتعيين أيقونة لـ **Game.com** باستخدام شاشة خصائص ملف الويندوز (*Windows file properties screen*).

4- نقوم بإرسال الملف **Game.com** كمرفق بريد إلكتروني إلى الضحية.

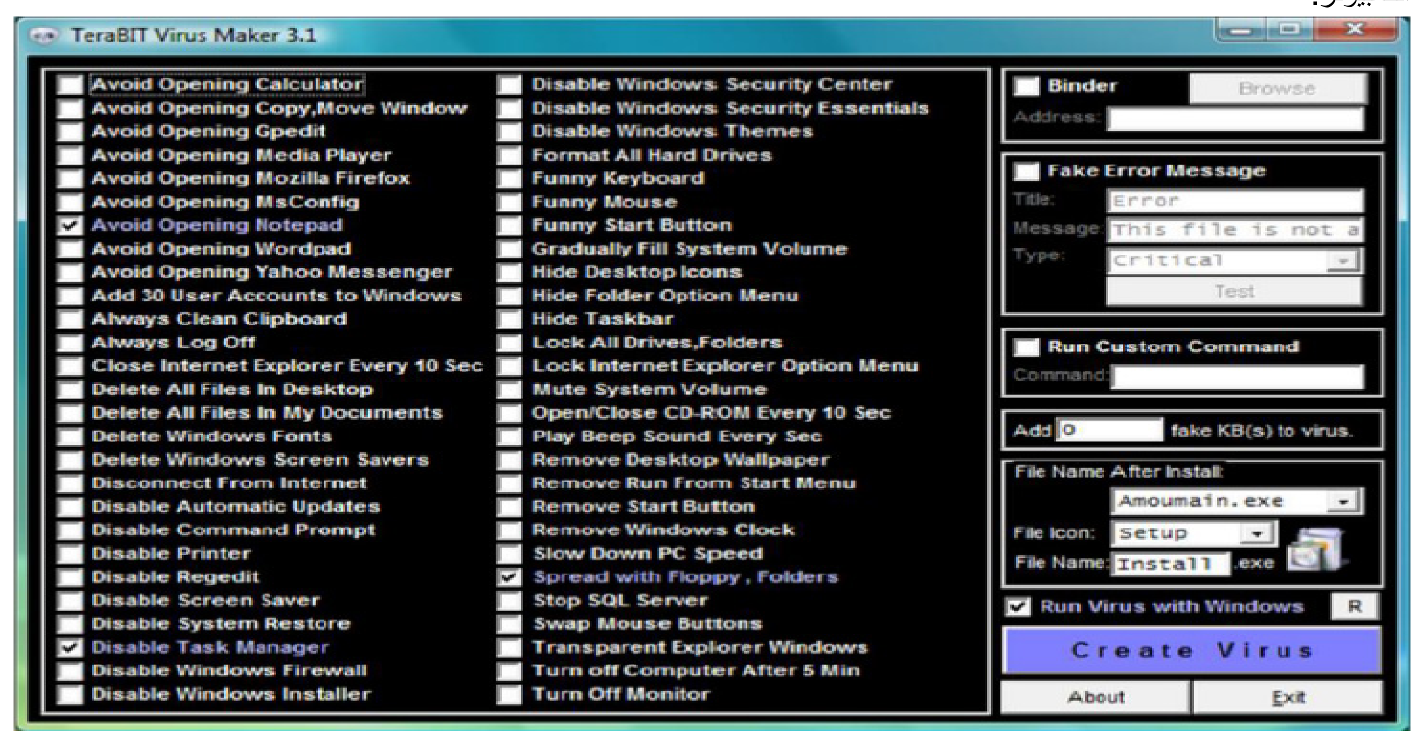
5- عند تشغيل الضحية هذا البرنامج، فهذا سوف يقوم بحذف الملفات الأساسية في المجلد(**\WINNT**)، مما يجعل الويندوز غير صالحة للاستعمال.

مما يجعل الضحية تضطر إلى إعادة تثبيت الويندوز، مما قد يسبب مشاكل لحفظ الملفات بالفعل.



TeraBIT Virus Maker

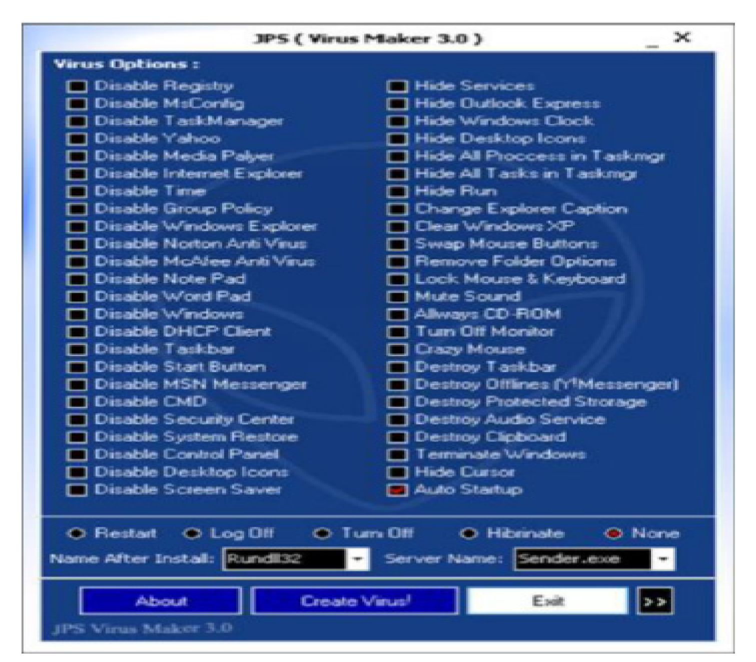
TeraBIT صانع الفيروسات هو فيروس الذى يتم الكشف عنه في الغالب من قبل برامج مكافحة الفيروسات عند فحصها. هذا الفيروس في الغالب لا يضر **PC**، لذلك يمكن تعطيل مكافحة الفيروسات المثبت على النظام لفترة قصيرة حتى تستطيع التعامل معه واستخدامه.
هذا البرنامج يقوم بصنع الفيروسات حسب نوع المهمة التي سوف يقوم بها الفيروس في جهاز الضحية ولا يحتاج الى تثبيت في جهاز الكمبيوتر.



JPS Virus Maker and DELmE's Batch Virus Maker

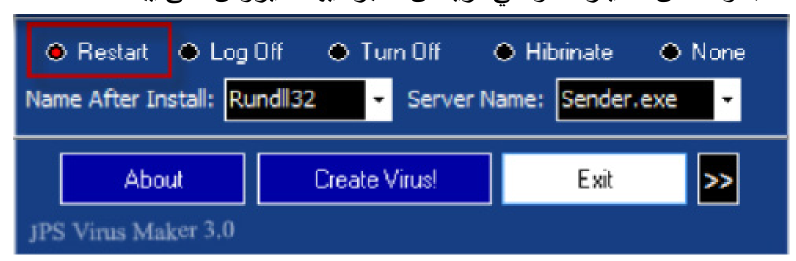
JPS Virus Maker

JPS Virus Maker هي أداة لإنشاء الفيروسات. كما أن لديها ميزة وهي تحويل الفيروس إلى دودة، ويمكن استخدامها لتعطيل الأجهزة العادية في النظام.

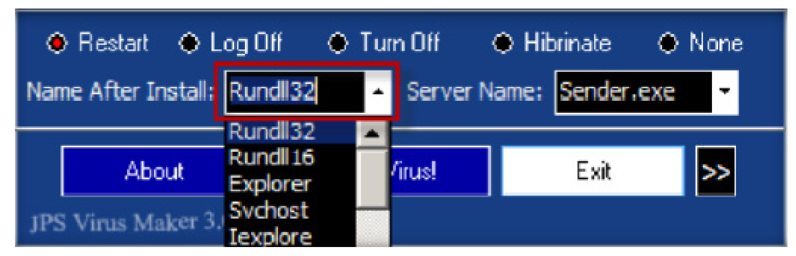


هذا البرنامج يقوم بصنع الفيروسات حسب نوع المهمة التي سوف يقوم بها الفيروس في جهاز الضحية ولا يحتاج الى تثبيت في جهاز الكمبيوتر. نجد أيضا انه يأتي معه العديد من الإمكانيات.

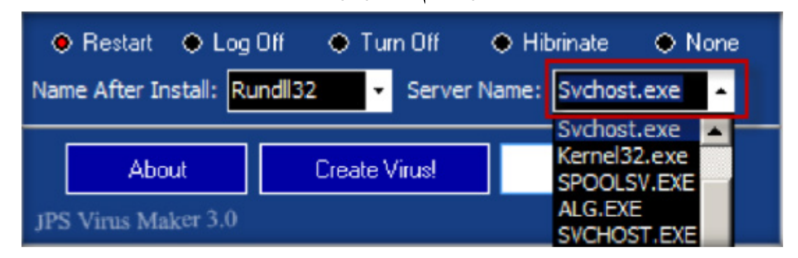
- نجد ان ما يلي النص **virus option** هي مجموعه من الخيارات التي تريد تضمينها في الفيروس الذي تريد إنشائه.
- نجد في القائمة السفلية مجموعه من الخيارات والتي تريد ان تخبر فيها الفيروس متى يبدا نشاطه.



- أيضا القائمة المنسدلة بجانب النص **Name After Install** والتي من خلالها تختار **service** التي سوف يظهر الفيروس كأنها هي.



- القائمة المنسدلة بجانب النص **Server Name** نختار اسم السيرفر.



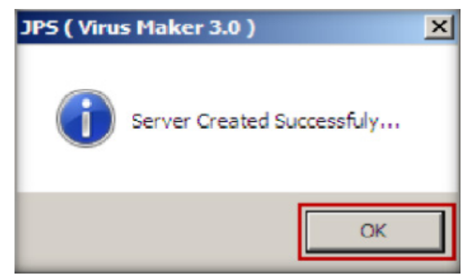
- قبل النقر فوق **Create Virus!** لإنشاء الفيروس يمكنك قبلها النقر فوق >> لتغير اعدادات الفيروس.



- والتي من خلالها يمكنك القيام بالعديد من الأشياء مثل تحويل الفيروس الى دوده، تغير كلمة المرور لويندوز **xp**، تغير اسم الكمبيوتر، تغير صفحة البداية الافتراضية لمتصفح المواقع الخاص بالضحية، تغير شكل ايقونة الفيروس وغيرها من الأشياء الأخرى.
- بعض الانتهاء من وضع اللمسات الأخيرة عليه يمكن الان النقر فوق **Create Virus!** لإنشاء الفيروس.

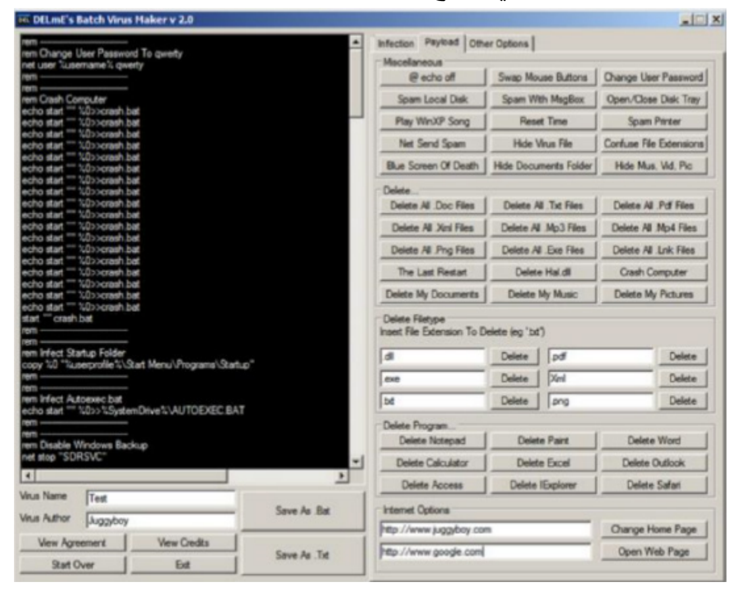


- عند انتهاء التطبيق من صنع الفيروس فسوف تظهر الرسالة التالية تخبرك بذلك.



DELmE's Batch Virus Maker

DELmE's Batch Virus Maker هو أداة بسيطة التي تسمح لك بإنشاء **bat file virus** من اختيارك لتتناسب مع المهام الخاصة بك.



Computer Worms 7.3

قبل هذا، كنا قد ناقشنا أنواع الفيروسات المختلفة. الآن سوف نناقش ديدان الكمبيوتر، وكيف أنها تختلف عن الفيروسات. يصف هذا القسم الديدان، وتحليل الدودة (**Stuxnet**)، وألية صنع الدودة (**Internet Worm Maker Thing**).

ديدان الكمبيوتر (Computer Worms)

ديدان الكمبيوتر (***Computer worms***) هي برامج صغيرة قائمة بذاتها غير معتمدة على غيرها تقوم بتكرار نفسها، وتنفيذ، وتنتشر عبر شبكة اتصالات مستقلة، دون تدخل الإنسان. صنعت للقيام بأعمال تدميرية أو لغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت أو إلحاق الضرر بهم أو بالمتصلين بهم، تمتاز بسرعة الانتشار ويصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة.

تصيب الدودة الحواسيب الموصولة بالشبكة بشكل اوتوماتيكي، ومن غير تدخل الإنسان وهذا الامر يجعلها تنتشر بشكل اوسع وأسرع عن الفيروسات. الفرق بينهم هو أن الديدان لا تقوم بحذف أو تغيير الملفات بل تقوم بتهليك موارد الجهاز واستخدام الذاكرة بشكل فظيع مما يؤدي إلى بطء ملحوظ جدًا للجهاز والاتصال بالشبكة. تختلف الديدان في عملها من نوع لآخر، فبعضها يقوم بالتناسخ داخل الجهاز إلى أعداد هائلة، بينما نجد بعضها يتخصص في البريد الإلكتروني بحيث تقوم بإرسال نفسها برسائل إلى جميع الموجودين بدفتر العناوين، بل أن البعض منها يقوم بإرسال رسائل قذرة لعددٍ عشوائي من المقيدين بسجل العناوين باسم مالك البريد مما يوقعه بالكثير من الحرج.

تكمن خطورة الديدان باستقلاليتها وعدم اعتمادها على برامج أخرى تلتحق بها مما يعطيها حرية كاملة في الانتشار السريع، وبلا شك أن هناك أنواعا منها غاية في الخطورة، حتى أصبح بعضها كابوساً مرعباً يلازم كل مستخدم للشبكة، كدودة **Tanatos** الشهيرة التي ظهرت خلال شهر أكتوبر 2002م وانتشرت انتشار النار بالهشيم وخلفت ورائها آثاراً تدميرية هائلة. تم استهداف الديدان ضد نظام التشغيل ويندوز، وأرسلت عن طريق البريد الإلكتروني، **IRC**، وظائف الشبكة الأخرى.

لا يتطلب لتكرار الدودة المضيف، وإن كان في بعض الحالات يمكن للمرء أن يقال بأن مضيف الدودة هي آلة أصيبت بذلك. الديدان هي نوع فرعي من الفيروسات. المهاجمين يستخدموا **worm payloads** لتثبيت **backdoor** في أجهزة الكمبيوتر المصابة، والتي تحولهم إلى **zombies** وينشأ **botnet**؛ هذه **botnet** يمكن استخدامها لتنفيذ المزيد من الهجمات الالكترونية.

ما هو الفرق بين الفيروس والديدان؟

Worms	Virus
الدودة، بعد أن يتم تثبيتها على النظام، يمكن نسخ ونشر نفسها باستخدام **IRC**، **Outlook**، أو غيرها من البرامج البريدية المعمول بها.	الفيروس هو ملف والذي لا يمكن أن ينتشر إلى أجهزة الكمبيوتر الأخرى ما لم يتم نسخ الملف المصاب ومن ثم إرساله إلى أجهزة الكمبيوتر الأخرى، في حين أن دودة يفعل عكس ذلك تماما.
الدودة عادة لا تقوم بتعديل أي من البرامج المخزنة.	ملفات مثل **.com**،**.exe**،**.sys**، أو مزيج منها تفسد بمجرد واحدة عمل الفيروس على النظام.
بالمقارنة مع الفيروس، الدودة يمكن إزالتها بسهولة من النظام.	الفيروسات هي أصعب بكثير في إزالتها من على الجهاز المصاب.
تحتوي على خيارات الانتشار أكثر من الفيروس	خيارات انتشارها أقل بكثير من الدودة لأن الفيروسات تصيب فقط الملفات الموجودة على الجهاز.





Worm Analysis: Stuxnet

المصدر: http://www.symantec.com/index.jsp

ستوكسنت أو ستكسنت (**Stuxnet**) هو فيروس كمبيوتري من الجيل الجديد قادر على التسلل إلى أنظمة التحكم والمراقبة المعلوماتية الخاصة بهذه المجمعات، وأيضاً بسواها من المجمعات التي تتحكم بالبنى التحتية في جميع البلدان الصناعية في العالم.

من الناحية التقنية فإنه فيروس من نوع "دودة" **worm** يصيب أنظمة **Windows**. وقد تم اكتشافه أولاً في حزيران\يونيو 2010 من جانب شركة **VirusBlokAda** المتخصصة في الأمن المعلوماتي، ومقرها في روسيا البيضاء. ثم ظهر في ماليزيا ودول متعددة، ويقدر أنها أصابت حوالي 45 ألف جهاز كمبيوتر في أنحاء العالم 60% في إيران وحدها و18% في اندونيسيا، ونحو2% في الولايات المتحدة. ويُعتقد أنه من صنع الولايات المتحدة الأمريكية وإسرائيل.

من الناحية العملية، إذا جاز التعبير، يقوم **Stuxnet** بأعمال تجسس على أنظمة التحكم الصناعية [***industrial control systems (ICS)***] وإعادة برمجتها. وقد تم برمجته خصيصا للهجوم على أنظمة (**SCADA**) المخصصة للمراقبة والتحكم وتجميع البيانات. ولدى **Stuxnet** القدرة على إعادة برمجة وحدات التحكم المنطقي القابلة للبرمجة[**Programmable Logic Controllers (PLCs)**] ، وإخفاء التغييرات التي تم تنفيذها. وتتم عملية الزرع الأول للفيروس بواسطة منافذ**USB** ، ومن ثم يتفشى بالأجهزة عن طريق التوالد المعروفة في الفيروسات الدودية.

نظام« **SCADA سكادا**» من تصميم شركة **Siemens** الألمانية، وله تطبيقات متعددة، كتنظيم حركة السير، وخطوط الأنابيب وإدارة المفاعلات النووية.

يتّفق العديد من الخبراء على أنّ **Stuxnet** قد صمّم في الأساس لضرب هدف صناعي محدّد، وتمكنوا من حصر هذا الهدف المحدد في المنشآت الإيرانيّة. وفي هذا الإطار، قدّم خبيران ألمانيّان نظريّتين متناقضتين حول الهدف المقصود. حيث أن النظرية الأولى تقول إن الهدف يمثّل مفاعل بوشهر النووي الإيراني المخطط لتشغيله. ويرى أنّ غاية زرع الفيروس ذات طبيعة تجسسيه، ويكمن في نقل المعلومات إلى كمبيوتر مركزي في ماليزيا. بينما تعتبر النظرية الأخرى أن مفاعل «نتانز» الإيراني أيضاً لتخصيب اليورانيوم، يشكّل هدفا أكثر جاذبيّة.

فلا تختصّ هذه الدودة بالتجسّس وحسب، وإنّما تحمل في طيّاتها مهمات تخريبيّة، كما تبيّن لجميع الاختصاصيين. إشارة إلى ورود معلومات تشير إلى أن الشيفرة المصدرية الخاصة بالفيروس تتضمن تاريخ "9أيار/مايو 1979"، وهو تاريخ إعدام جاسوس يهودي إيراني في إيران، بعد إنشاء "الجمهورية الإسلامية الإيرانية".

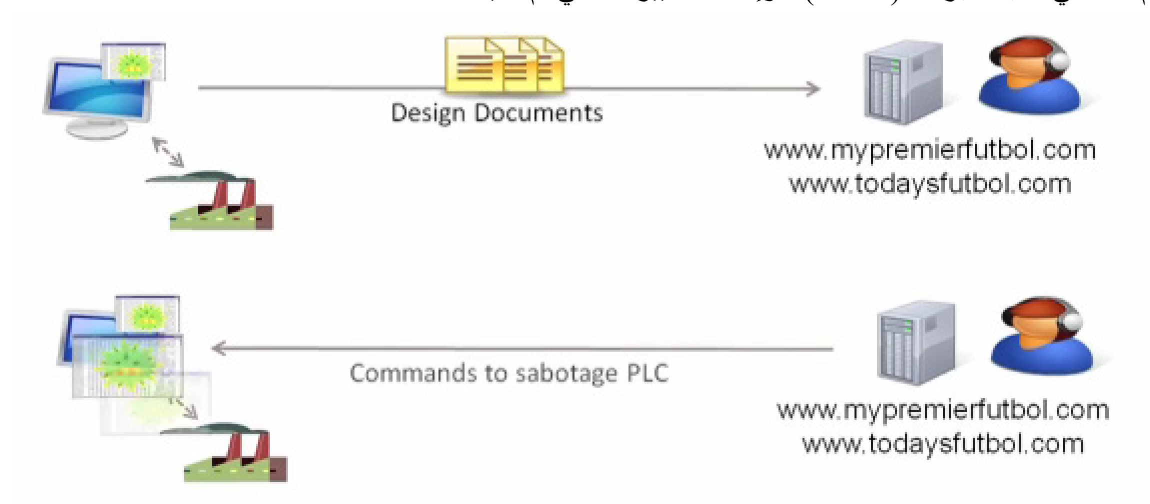
والمعروف أن لدى القوات المسلحة "الإسرائيلية" وحدة متخصصة في الحرب المعلوماتية تعرف بالوحدة 8200، ولهذه الوحدة القدرات التي تتيح لها تطوير فيروس مثل الـ**Stuxnet** . ولم تنفِ "إسرائيل"، كما أنها لم تؤكد الشكوك المحيطة بالدور الذي ذُكر بأنها اضطلعت فيه بهذا الشأن. وقد وصفت شركة الأمن الرقمي **Kaspersky Labs** الفيروس **Stuxnet** بأنه "نموذج عامل ومخيف ومن شأنه أن يخلق سباق تسلح جديد في العالم". وأشارت إلى خبراء يعملون لحساب دولة ما أو مجموعات لديها قدرات تمويلية عالية وراءه.

معلومات عن اختبار الفيروس في أميركا: ومن الأمور المثيرة التي لم تذكرها سوى قلة نادرة من وسائل الإعلام هو أن هناك دلائل كثيرة تشير إلى أنه ربما جرى اختبار هذا الفيروس في الولايات المتحدة الأميركية قبل توجيهه إلى إيران، وأن هذا الاختبار قد يكون تسبب بنتائج مدمرة. فلقد حصل تفجير دمر مجمع سكني جنوبي ولاية كاليفورنيا الأميركية في 9 أيلول/سبتمبر 2010 بسبب انفجار أنابيب شبكة الغاز التي كانت تغذي هذا المجمع، ولم يتم تحديد أسباب هذا الانفجار بدقة، لكن الخبراء يرجحون بأنه قد يعود إلى خلل في نظام تحكم ومراقبة شبكة الأنابيب، أي أن الفيروس كان يمكن أن يتسبب بالحادث...

كذلك، فإن السبب الحقيقي لانفجار محطة استخراج النفط في خليج المكسيك في 20 نيسان/أبريل الجاري لم يعرف بعد، ولكنه قد يعود أيضاً إلى خلل في نظام التحكم والمراقبة. وقد أوردت النشرة الأميركية "صحافة أميركا الحرة" **American Free Press** الشكوك والقرائن حول احتمال أن يكون "الإسرائيليين" قد اختبروا الفيروس **Stuxnet** على حساب الولايات المتحدة في عدده 42.

ستكسنت يقوم بمهاجمه أنظمة التحكم الصناعية [**industrial control systems (ICS)**] المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا حيث لا يعمل بشكل عشوائي كما هي العادة وإنما بشكل محدد جدا وذلك عن طريق التعديل على **Programmable Logic Controllers (PLCs)**. إذ يقوم بعد اختراق الأجهزة والحواسيب بالتفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة سيمنز الألمانية(**Siemens Step7 software**) ، وفي حاله ما وجدها عندها يقوم بتفعيل نفسه ويبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة من خلال العبث بأنظمة التحكم وقد تتعدد المنشآت التي يستطيع مهاجمتها من خطوط نقل النفط إلى محطات توليد الكهرباء وحتى المفاعلات النووية وغيرها من المنشآت الاستراتيجية الحسّاسة، أمّا إذا لم يجدها، فيترك الحاسوب وشأنه.

قد تمت برمجة ستكسنت خصيصا للهجوم على برنامج «سيماتيك وين سي سي»، وهو ما يسمى بنظام سكادا (**SCADA**) أو «التحكم الإشرافي وجمع المعطيات»، وهو مصمم من شركة سيمنز الألمانية لاستخدامات متعددة، كتنظيم حركة السير، السيطرة على خطوط تجميع آلات المصنع، وخطوط الأنابيب وإدارة المفاعلات النوويّة وغيرها من المهام التي يتم القيام بها آلياً. ولدى ستكسنت القدرة على إعادة برمجة وحدات التحكم المنطقي القابلة للبرمجة(**PLCs**) ، وإخفاء التغييرات التي تم تنفيذها.



قد قامت شركة سيمنز منذ اكتشافها لهذه الدودة الجديدة بحملة واسعة لتعقّب انتشارها عبر موقعها الإلكتروني.

شركة الأمن الرقمي الروسية "مختبرات كاسبرسكي" **Kaspersky Laboratories**" وصفت **Stuxnet** بأنه "نموذج عامل ومخيف ومن شأنه أن يخلق سباق تسلح جديد في العالم". واشارت إلى أنه يوجد خبراء يعملون لحساب دولة ما أو مجموعات لديها قدرات تمويلية عالية وراءه.

ورد أن ستكسنت دمرت نحو خمس من أجهزة الطرد المركزي النووي الإيراني.

ستكسنت يحتوي على العديد من الميزات مثل:

- يعيد إنشاء نسخ ذاتيا من خلال محركات الأقراص القابلة للإزالة باستغلال نقاط ضعف للسماح بالتنفيذ اليا (**auto-execution**).
- ينتشر في الشبكة المحلية من خلال ثغرة أمنية في نظام التشغيل **Windows** في **Windows Print Spooler**.
- ينتشر عن طريق **SMB** من خلال استغلال**Microsoft Windows Server Service RPC** من خلال التعامل مع ثغرة **Remote Code Execution**.
- تنسخ وتنفذ نفسها على أجهزة الكمبيوتر عن بعد عن طريق مشركات الشبكة (***network share***) والتي تقوم بتشغيل الخادم **WinCC database server**.
- ينسخ نفسه إلى **Step 7 projects** بمثل الطريقة التي يتم تنفيذها تلقائيا عند يتم تحميل**Step 7 project** .
- يقوم بتحديث نفسه من خلال آلية **peer-to-peer** ضمن **LAN**.
- يستغل أربعة نقاط ضعف **unpatched** لمايكروسوفت.
- يتصل بخادم القيادة والتحكم (***command and control server***) التي تسمح للهاكر بتحميل fوتنفيذ التعليمات البرمجية، بما في ذلك الإصدارات المحدثة.
- يحتوي على **rootkit windows** الخفية التي تخفي الثنائيات (***binary***)الخاصة به في محاوله لتجاوز المنتجات الأمنية.

ستكسنت لديه ثلاث وحدات: **worm** الذي تنفذ كافة الإجراءات التي تتعلق بـ **payload** الرئيسية للهجوم؛ **links files** والذي ينفذ نشر نسخ الدودة تلقائيا؛ وعنصر **rootkit** المسؤولة عن إخفاء كل الملفات والعمليات الخبيثة، ومنع الكشف عن وجود ستكسنت. عادة يتم أدخال ستكسنت للبيئة الهدف عن طريق محرك أقراص فلاش **USB** المصابة. الفيروس ينتشر عبر الشبكة ويفحص البرمجيات للبحث عن سيمنز **STEP7** على أجهزة الكمبيوتر التي تسيطر على **PLC**. في غياب كل المعايير، ستكسنت يصبح نائم داخل الكمبيوتر. إذا توفرت الشروط على حد سواء، فان ستكسنت يقوم بزرع **rootkit** المصابة على برنامج **PLC** و**STEP7**، ومن ثم تعديل القوانين وإعطاء أوامر غير متوقعة لـ **PLC**.

ستكسنت يتكون من ملف (**.dll**) كبير يحتوي على العديد من (**export**) والموارد(**resource**) المختلفة واثنين من كتل الاعداد المشفرة (***encrypted configuration blocks***). فإنها تتصيد **Ntdll.dll** لمراقبة الطلبات لتحميل أسماء الملفات التي وضعت خصيصا (***specially crafted filenames***)؛ يتم تعيين هذه الأسماء لموقع آخر بدلا من، الموقع المحدد بواسطة **W32.Stuxnet**. **المكون الساقط** (***dropper component***) للستكسنت هو برنامج الغلاف (**wrapper program**) الذي يحتوي على كافة العناصر المخزنة داخل نفسها تحت القسم المسمى **".stub"**، وعندما يتم تنفيذ هذا التهديد، فان برنامج الغلاف (***wrapper program***) يستخرج ملفات (**.dll**) من القسم **.sub**، ثم يقوم بتعينه او زراعته في الذاكرة كوحدة نمطية، والتي تقوم باستدعاء واحدة من **export**. عندما يتم استدعاء (**export**)، فان ستكسنت عادة يقوم بحقن **.dll** بأكمله إلى عمليات أخرى ثم يستدعى فقط **export** معينة. عندما يتم الحقن في عملية موثوق بها، فان ستكسنت يتحفظ بأكواد الحقن في عملية موثوق به أو يرشد العملية الموثوق بها لحقن الكود في عملية أخرى قيد التشغيل حاليا. ويستخدم طريقة خاصة مصممة لتجاوز **behavior blocking** و **Host intrusion-protection based technologies**والتي ترصد تحميل **library calls**.

الدول التي تأثرت

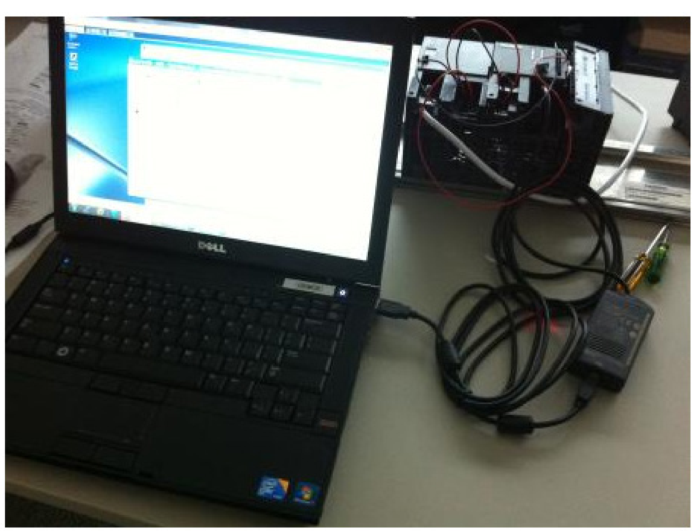
يعتقد أن هجوما إلكترونية من جهة ما قد شن باستخدام فيروس ستوكسنت على أنظمة المعلومات في إيران وخصيصا لإلحاق الضرر بأجهزة الطرد المركزي لتخصيب اليورانيوم في المنشآت النووية الإيرانية. وكان يستهدف على ما يبدو البرنامج النووي الإيراني ككل. ثم ظهر في ماليزيا ودول متعددة، ويقدر انها اصابت حوالي 45 ألف حاسب الي في أنحاء العالم 60% في إيران وحدها و18% في اندونيسيا، ونحو2% في الولايات المتحدة.

Infection Routine Flow

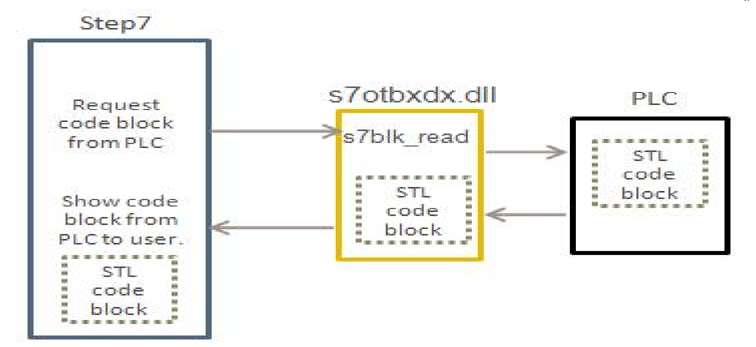
قبل مناقشة تقنيات ستكسنت لمهاجمة **PLCs** أولا سوف نقدم نظرة على أساسيات كيفية الوصول إلى **PLCs** العامة وبرمجتها.



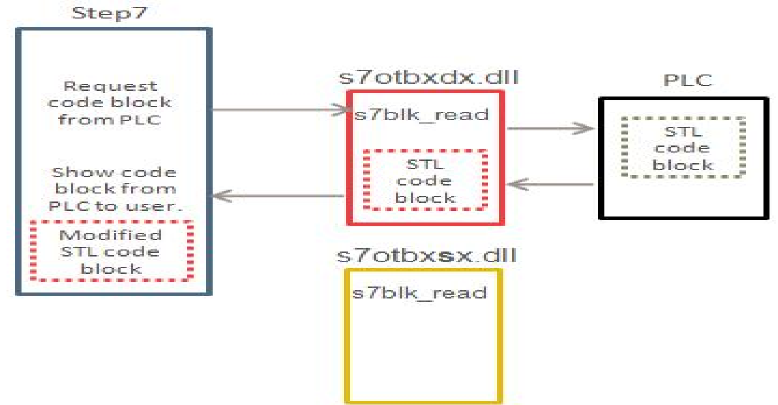
للوصول إلى **PLCs**، فانه يحتاج الى برامج معينة ليتم تثبيتها؛ ستكسنت تستهدف على وجه التحديد التطبيق **WinCC/Step 7** المستخدم لبرمجة نماذج معينة من **PLCs**. مع هذا البرنامج، يمكن للمبرمج الاتصال بـ **PLCs** عن طريق كابل البيانات والوصول إلى محتويات الذاكرة، وإعادة تكوين ذلك، تحميل البرنامج عليه، أو تصحيح اكواد تم تحميلها سابقا. بمجر ان يتم اعداد **PLCs** وبرمجته، فيمكنك فصل آلة الويندوز و**PLCs** سوف يعمل من تلقاء نفسه. لإعطائك فكرة عما يبدو هذا مثل ما في الحياة الحقيقية، وهنا صورة لبعض المعدات الأساسية الاختبار في المختبر:



البرنامج **Step 7** يستخدم ملف مكتبة (**library file**) يسمى **s7otbxdx.dll** لأداء التواصل الفعلي مع **PLC**. ويدعو البرنامج **STEP7** إجراءات مختلفة في هذا **DLL** عندما يريد الوصول إلى **PLC**. على سبيل المثال، إذا كان كتلة من الأكواد تقرأ من **PLC** باستخدام **Step 7**، فانه روتينيا يتم استدعاء **s7blk_read**. الأكواد في **s7otbxdx.dll** تقوم بالوصول إلى **PLC**، تقرأ الأكواد وتمررها إلى البرنامج **STEP7**، كما هو مبين في الرسم البياني التالي:



دعونا الآن نلقي نظرة على كيف يعمل الوصول إلى **PCL** عند تثبيت ستكسنت. عندما يعمل ستكسنت، فانه يعيد تسمية الملف الأصلي **s7otbxdx.dll** إلى **s7otbxsx.dll**. بعد ذلك يستبدل **DLL** الأصلية مع نسخته الخاصة باستخدام تقنيات الحقن (***injection technique***). ستكسنت يمكن الآن اعتراض أي **calls (استدعاء)** يتم إجراؤها للوصول إلى **PLCs** من أي حزم من البرامج.



نجدا ان ملف ستكسنت **s7otbxdx.dll** المعدل يحتوي على جميع الصادرات (**export**)المحتملة لـ**DLL** الأصلي -بحد أقصى **109** -مما يسمح لها التعامل مع جميع الطلبات نفسها. يتم توجيه غالبية هذه **export** ببساطة إلى **DLL** الحقيقية، التي تسمى الآن **s7otbxsx.dll**، ولا شيء غير مرغوب فيه يحدث؛ في الواقع، **93** من أصل **109** من **export** يتم التعامل معها بهذه الطريقة. الخدعة هنا، تكمن في الصادرات **16** التي لا يتم توجيهها ببساطة ولكن بدلا من ذلك يتم اعتراضها من قبل **DLL** المعدل الخاص بستكسنت. الصادرات 16 (**export**) التي اعترضت هي عباره عن إجراءات القراءة والكتابة، وتحديد كتل التعليمات البرمجية على **PLCs**. عن طريق اعتراض هذه الطلبات ستكسنت هو قادرا على تعديل البيانات المرسلة إلى أو العائدة من **PLC** من دون أن يدرك مشغل **PCLs**. كما أنه من خلال هذه الإجراءات ستكسنت قادر على إخفاء الشيفرات الخبيثة التي هي في **PLCs**.

ستكسنت يقوم أولا بفحص ما إذا كان لديها امتيازات المسؤول على الكمبيوتر. ستكسنت تريد أن تعمل مع أعلى امتيازات ممكنه حتى يتسن له اتخاذ الإجراءات التي يريدها على الكمبيوتر. أما إذا لم يكن لديه امتيازات المسؤول، فإنه ينفذ واحد من اثنين من هجوم تصعيد الامتيازات **zero-day** كما هو موضح في الرسم البياني التالي.

إذا كانت العملية بالفعل لديها الحقوق التي تطلبها، فإنها تشرع في الاستعداد لاستدعاء الصادرات 16 في الملف(**.dll**) الرئيسي. عندما لا يكون لدى العملية امتيازات المسؤول على النظام، فإنه يحاول اكتساب هذه الامتيازات باستخدام واحد من اثنين من هجوم تصعيد الامتيازات **zero-day**. ويستخدم ناقلات الهجوم (***attack vector***) مستندا على نظام التشغيل الموجود على الكمبيوتر المخترق. إذا كان نظام التشغيل **ويندوز فيستا، ويندوز 7، أو Windows Server 2008 R2**، فان يستغل ثغرة **Task Scheduler** لرفع امتيازاته. أما إذا كان نظام التشغيل **windows xp** فان يستغل الثغرة **win32k.sys** لرفع امتيازاته.

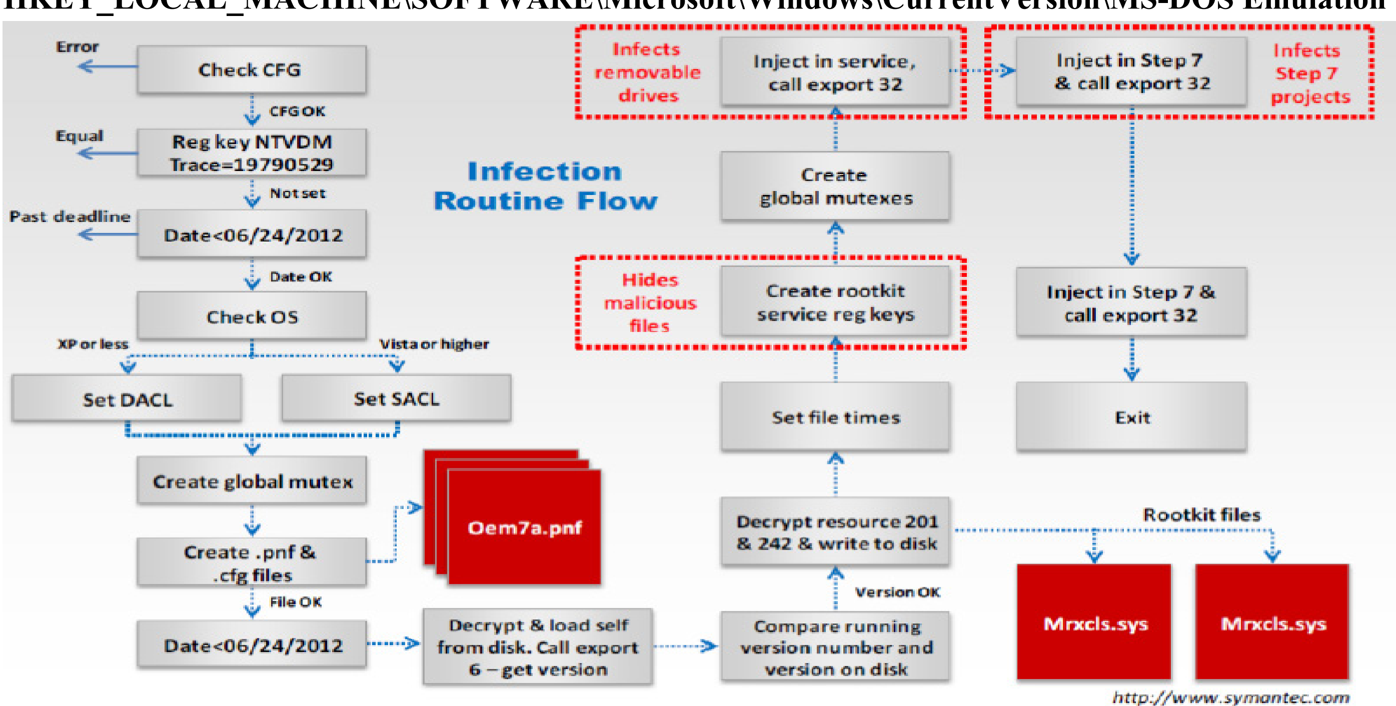
إذا تم استغلال، كل من هذه الثغرات بشكل رئيسي. فان ملف **DLL** يتم تشغيله كأنه عملية جديده، سواء داخل عملية **Csrss.exe** في حالة كانت الثغرة **win32k.sys** أو مهمة جديدة مع امتيازات المسؤول في حالة الثغرة **Task Scheduler**.

الأكواد التي تستغل الثغرة **win32k.sys** يتم تخزينها في **resource 250**. إن تفاصيل ثغرتي **win32k.sys** و**Task Scheduler** حاليا لم يتم الافراج عن **patch** لها وليست متاحة بعد.

كما قلنا سابقا ان الإصدارات 16 الباقية هي التي يتحكم فيها ستكسنت، بعدا اكتمال فحص ستكسنت للصادر (**export**)رقم 15 فانه يبدا استدعاء الصادر رقم 16.

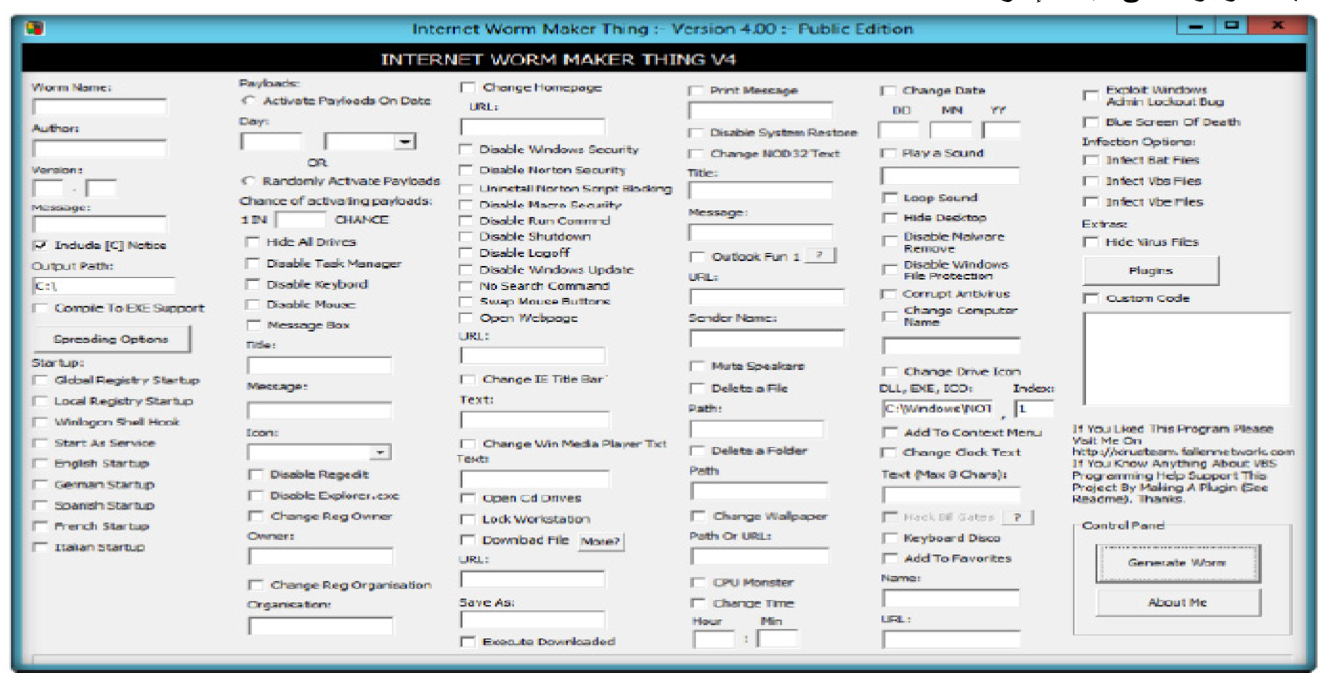
الصادر رقم 16 (**export 16**) هو المثبت الرئيسي للستكسنت. فإنه يتحقق من تاريخ ورقم الإصدار من الكمبيوتر المخترق؛ يفك شفرة، وينشا، ويثبت ملفات **rootkits** ومفاتيح **registry**؛ يحقن نفسه في عملية **Services.exe** ليصيب محركات الأقراص القابلة للإزالة؛ يحقن نفسه في عملية**STEP7** ليصيب كل **STEP7 Project**؛ يقوم بتثبيت كائنات المزامنة العالمية (***global mutexes***) التي تستخدم للاتصال بين المكونات المختلفة؛ ويربطه إلى ملفRPC . **Export16** يقوم أولا بفحص هل بيانات التكوين صالحه، وبعد ذلك فإنه يتحقق من قيمة **"NTVDM TRACE"** في مفتاح **registry** التالي:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS Emulation



Worm Maker: Internet Worm Maker Thing

Internet Worm Maker Thing هي أداة مصممة خصيصا لأنشاء دودة. الديدان الانترنت هذه التي تم إنشائها تحاول النشر أكثر على الشبكات التي هي في الأساس **preset invasion proxy attacks** التي تستهدف المضيف من الناحية الفنية، تسمه **poison**، وتصنع قاعدة وخطط لشن هجوم في المستقبل. الديدان تعمل بشكل مستقل. دودة الإنترنت ترسل نسخ عن نفسها عبر أجهزة الكمبيوتر الضعيفة الموجودة على شبكة الإنترنت.



Malware Analysis 7.4

تحليل البرمجيات الخبيثة (**Malware Analysis**) يعرف بانه عملية أخذ البرمجيات الخبيثة بشكل منفصل لدراسته. عادة ما يتم تنفيذ ذلك لأسباب مختلفة مثل لإيجاد نقاط الضعف التي يتم استغلالها لنشر البرمجيات الخبيثة، المعلومات التي سرقت، تقنيات الوقاية التي يجب اتخاذها ضدها من دخول النظام أو الشبكة في المستقبل. هذا الجزء يفسر معلومات مفصلة حول إجراء تحليل للبرمجيات الخبيثة في الشرائح القليلة المقبلة.

What Is a Sheep Dip Computer?

Sheep dipping يشير إلى تحليل الملفات المشتبه به، والرسائل الواردة، وغيرها من أجل البرمجيات الخبيثة.

Sheep dip computer هو جهاز كمبيوتر مخصص يستخدم لاختبار الملفات على الوسائط القابلة للإزالة من اجل الفيروسات قبل السماح له ليتم استخدامها مع أجهزة الكمبيوتر الأخرى.

هذا **"Sheep dipping computer"** يتم عزل الكمبيوتر عن أجهزة الكمبيوتر الأخرى على الشبكة لمنع أي من الفيروسات من دخول النظام. قبل اتمام هذا الإجراء، فانه يتم حفظ أي من البرامج التي تم تحميلها على وسائط خارجية مثل الأقراص المدمجة أو الأقراص المرنة.

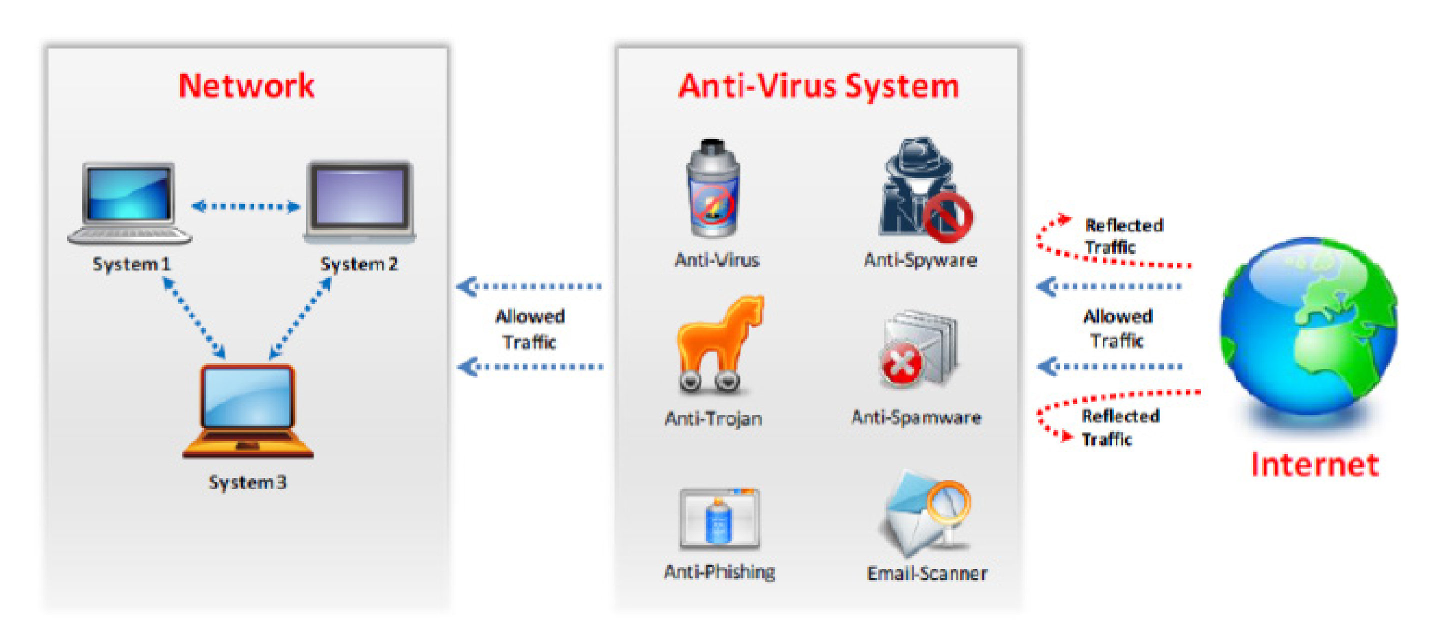
Sheep dip computer يتم تثبيت فيه مراقب المنافذ، مراقب الملفات، مراقب الشبكة، وبرامج مكافحة الفيروسات ويتم ربطة بالشبكة في ظل ظروف خاضعة لرقابة صارمة.

Sheep dip computer

- يقوم بتشغيل مراقب المنافذ والشبكة.
- يقوم بتشغيل مراقب اذونات المستخدم والجروب، مراقب العملية.
- تشغيل مراقب برامج الأجهزة (*device driver*) ومراقب الملفات.
- تشغيل مراقب **registry** والكيرنل.

أنظمة استشعار مكافح الفيروسات (Antivirus Sensor Systems)

نظام مكافحة الفيروسات هي عبارة عن مجموعة من برامج الكمبيوتر التي يكتشف ويحلل مختلف تهديدات الشيفرات الخبيثة مثل الفيروسات، والديدان، وأحصنة طروادة. يتم استخدامها جنبا إلى جنب مع أجهزة **Sheep dip computer**.



ويشمل نظام مكافحة الفيروسات مكافحة الفيروسات(**anti-virus**)، مكافح التجسس(**anti-spyware**)، مكافحة طروادة(**anti-Trojan**)، **anti-spamware**، **anti-Phishing**، وفاحص البريد الإلكتروني، وهلم جرا. عادة، يتم وضعها فيما بين الشبكة والإنترنت. لأنها تتيح فقط الحركة الحقيقية (**genuine traffic**) الوحيدة في التدفق من خلال الشبكة وغلق حركة المرور الضارة من الدخول. ونتيجة لذلك، فإنه يضمن أمن الشبكة.

Malware Analysis Procedure: Preparing Testbed (إجراء تحليل البرامج الضارة)

تحليل البرمجيات الخبيثة يقدم فهم عميق لكل عينة على حدة ويحدد الاتجاهات الفنية الناشئة من مجموعات كبيرة من عينات البرمجيات الخبيثة. عينات البرامج الضارة هي في معظمها متوافقة مع **windows binary executable**. يجري تحليل البرمجيات الخبيثة مع مجموعة متنوعة من الأهداف. فيما يلي هو الإجراء المتبع لتحليل البرامج الضارة لإعداد مختبر:

- تثبيت برنامج **VMWare** أو **Virtual PC** أو **Oracle VM** على النظام.
- تثبيت نظام التشغيل المضيف على**Virtual PC/VMWare** .
- عزل هذا النظام عن الشبكة من خلال ضمان أن بطاقة **NIC** في الوضع "**host only**".
- تعطيل المجلدات المشتركة (**shared folders**) وعزل الضيوف(**guest isolation**) .
- نسخ البرامج الضارة الى نظام التشغيل المضيف.

اجراء تحليل البرامج الضارة (Malware Analysis Procedure)

- الخطوة 1: إجراء تحليل ثابت (**static analysis**) عندما تكون البرمجيات الخبيثة غير نشطه.
- الخطوة 2: جمع المعلومات حول:

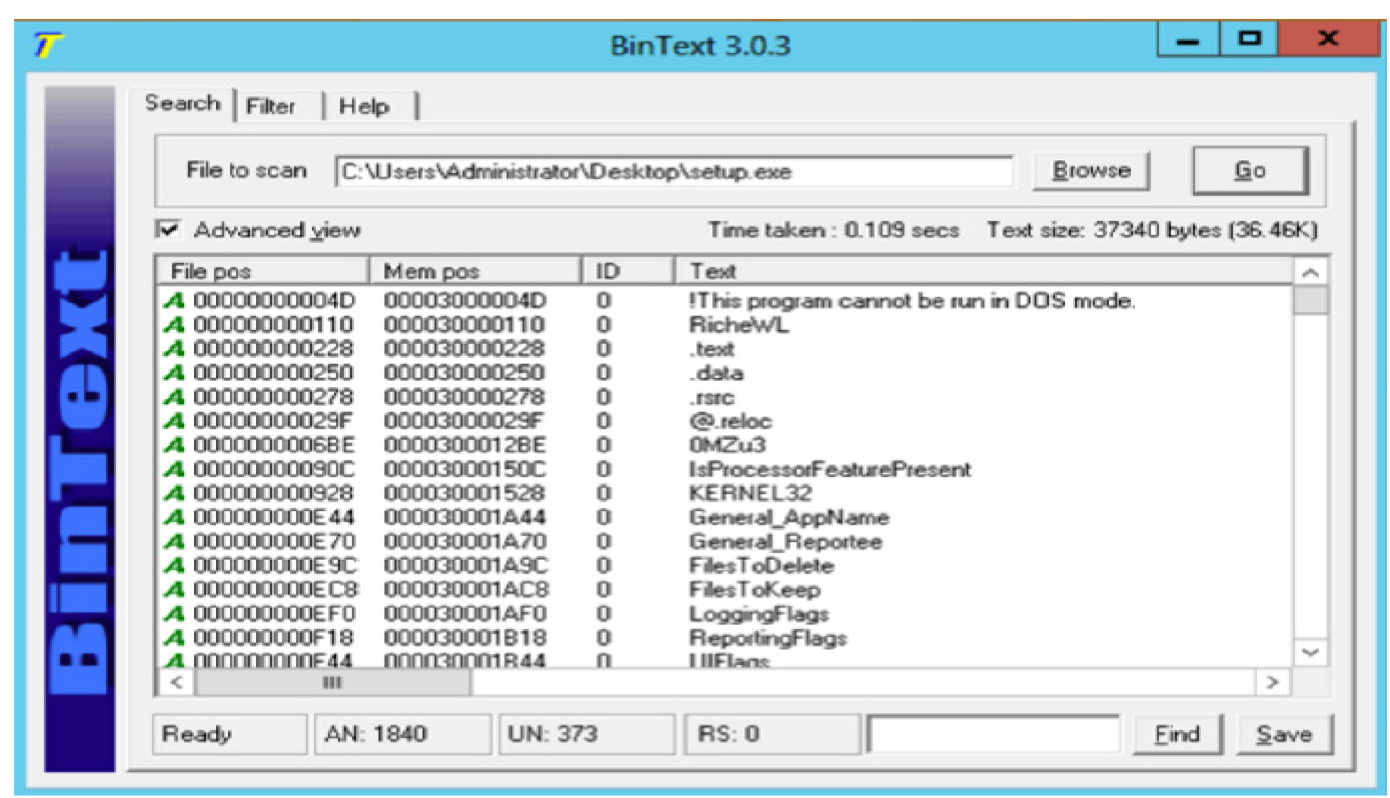
  قيم **string** التي وجدت في **binary** مع مساعدة من أدوات استخراج **string** مثل **BinText**.

  تقنية التعبئة والضغط المستخدمة مع مساعدة من أدوات الضغط وإزالة الضغط مثل**UPX** .

BinText

المصدر http://www.mcafee.com/us

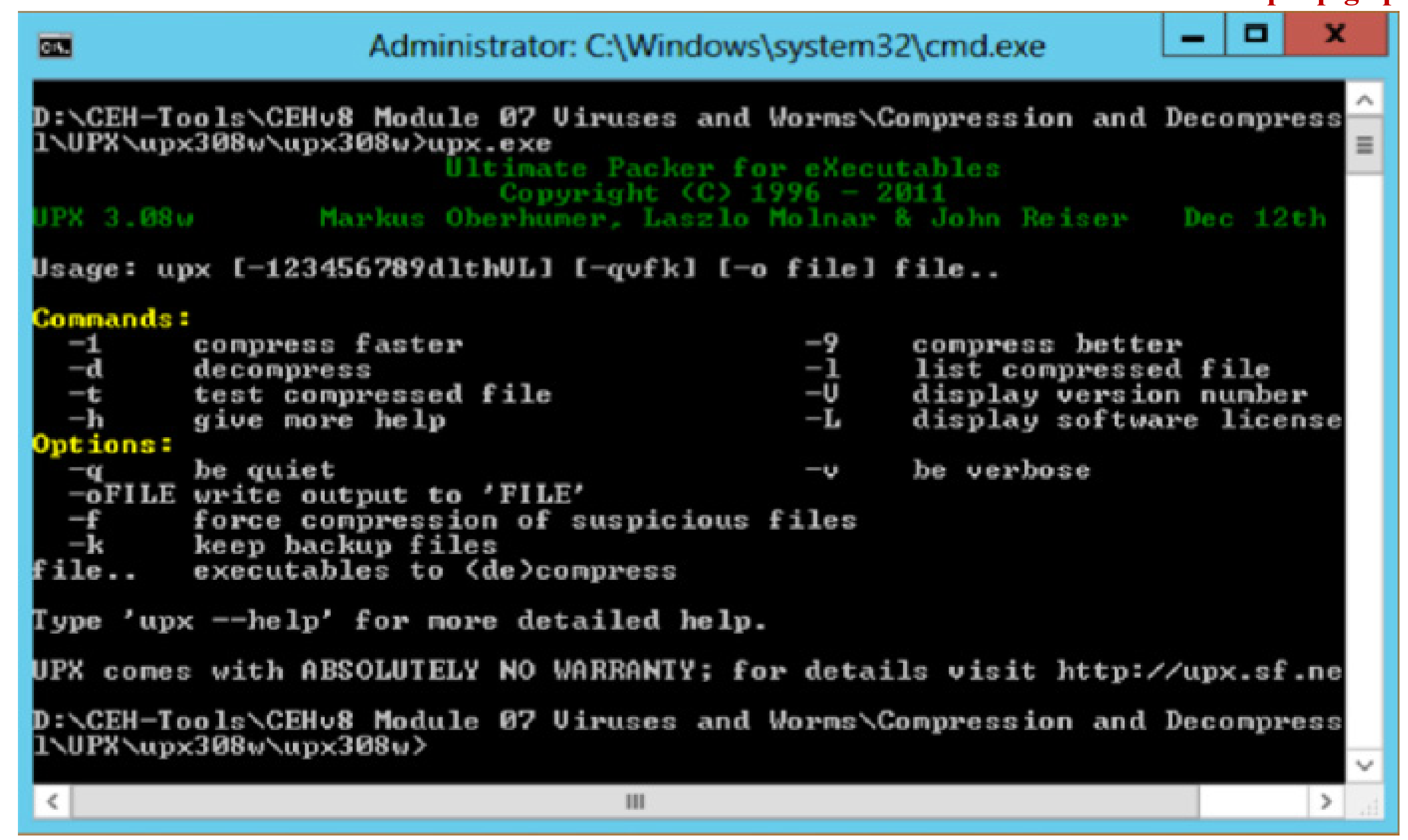
BinText يمكنه استخراج النص من أي نوع من الملفات، وتشمل القدرة على العثور على نص **ASCII** عادي، نص يونيكود (**ANSI** مزدوج البايت) ، **resource strings**، وتوفير معلومات مفيدة لكل عنصر في الاختيار "**advanced**" في وضع العرض.



UPX

المصدر: http://upx.sourceforge.net

UPX يحقق نسبة ضغط ممتازة (**excellent compression ratio**) وسريعة جدا في فك الضغط. انها عادة أفضل من برنامج ضغط **WinZip/zip/gzip**.

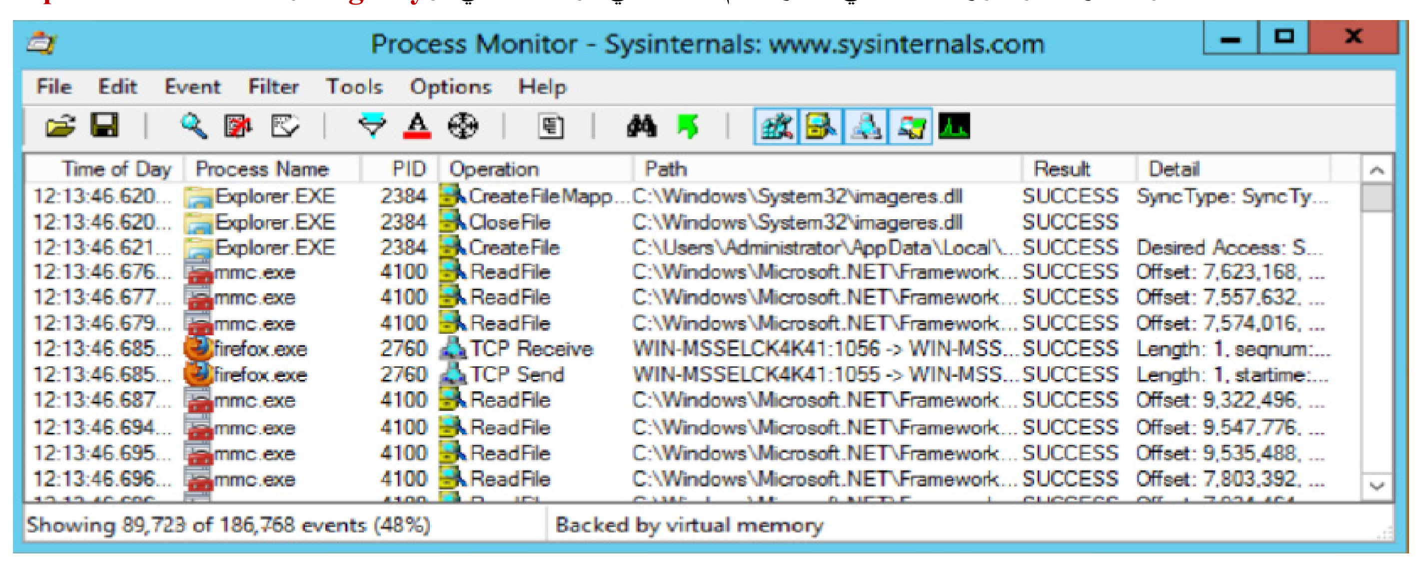


- الخطوة 3: إعداد اتصال الشبكة والتحقق من أنه لن يعطي أي أخطاء.
- الخطوة 4: تشغيل الفيروس ورصد العمليات ونظام المعلومات بمساعدة أدوات لرصد العمليات مثل **Process Monitor** و**Process Explorer**.

Process Monitor

المصدر: http://technet.microsoft.com/en-US

Process Monitor هو أداة رصد ويندوز متقدمة التي تظهر نظام الملفات في الوقت الحقيقي، و**registry**، ونشاط **process/thread**.

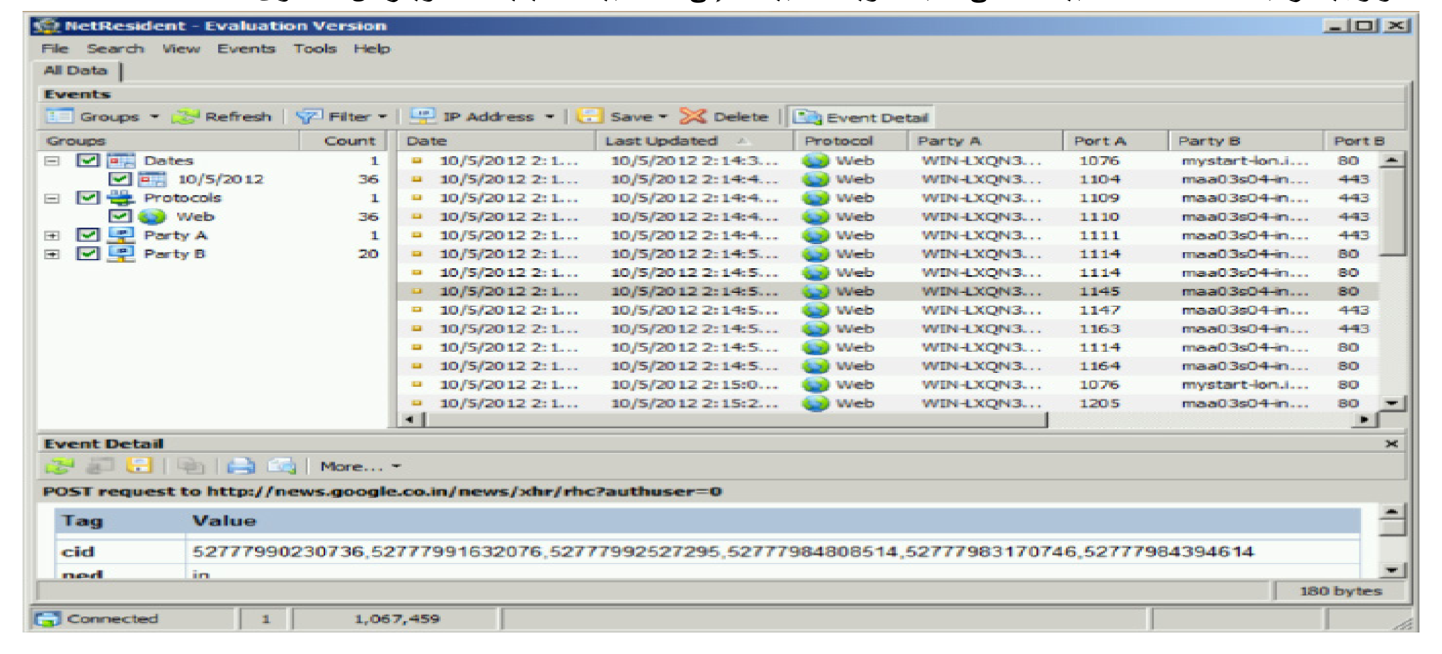


- الخطوة 5: تسجيل معلومات حركة مرور الشبكة باستخدام أدوات الاتصال ورصد محتوى الحزمة مثل **NetResident** و**TCPView**.
- الخطوة 6: تحديد الملفات المضافة، العمليات التي أنشئت، التغييرات على **registry** مع مساعدة من أدوات رصد السجل مثل **Regshot**

NetResident

المصدر: http://www.tamos.com

NetResident هو تطبيق لتحليل محتوى الشبكة مصمم لرصد وتخزين وإعادة بناء مجموعة واسعة من الأحداث وأنشطة الشبكة، مثل رسائل البريد الإلكتروني، صفحات الويب، الملفات التي تم تحميلها، الرسائل الفورية، والمحادثات عبر بروتوكول الإنترنت. فإنه يستخدم تكنولوجيا مراقبة متقدمة لالتقاط البيانات على الشبكة، ويحفظ البيانات إلى قاعدة بيانات، يعيد ذلك، ويعرض المحتوى.

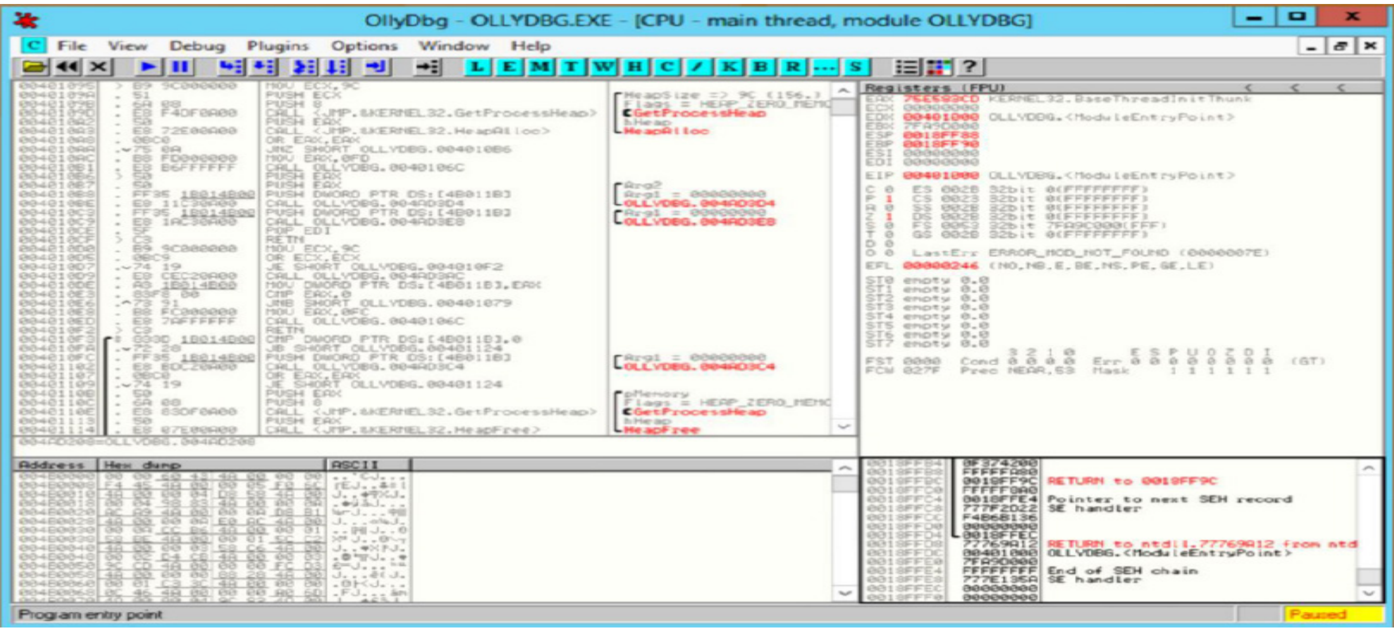


- الخطوة 7: جمع المعلومات التالية باستخدام أدوات التصحيح (**debugging**)مثل **ollyDbg** و **ProcDump**.
  - ❖ طلبات الخدمة (**Service requests**).
  - ❖ محاولات الاتصالات الواردة والصادرة(***Attempts for incoming and outgoing connections***) .
  - ❖ معلومات الجداول**DNS** .

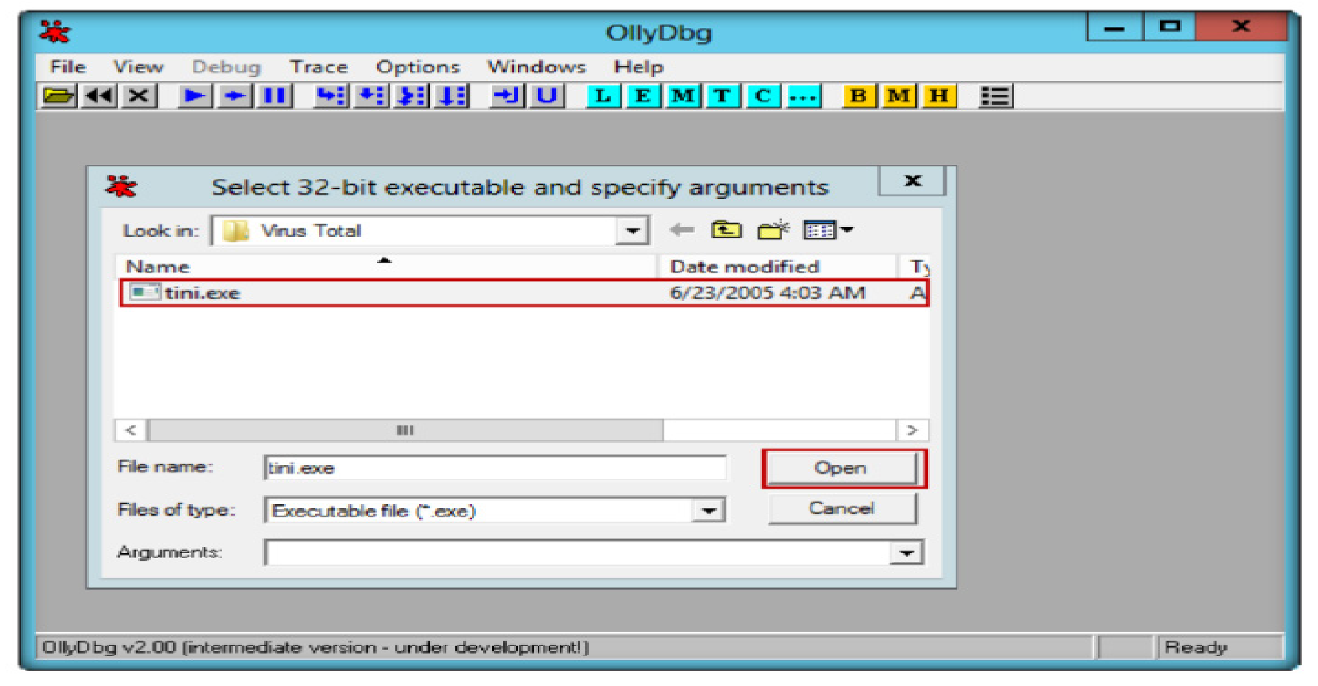
OllyDbg

المصدر: http://www.ollydbg.de

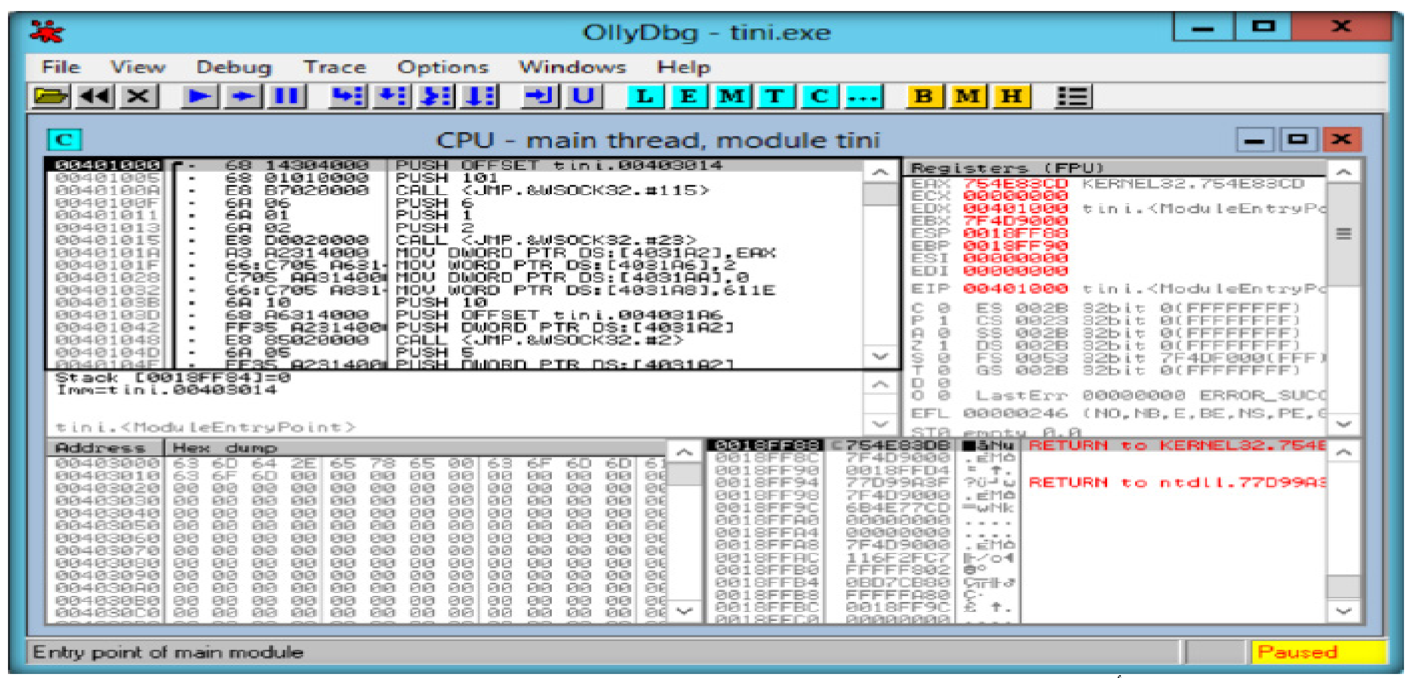
OllyDbg هو 32-بت محلل التصحيح على مستوى لغة التجميع (**assembler level analyzing debugger**) لمايكروسوفت ويندوز. لتحليل الأكواد الثنائية (**binary code**) والتي يجعلها مفيدة بشكل خاص في الحالات التي يكون فيها المصدر غير متوفر.



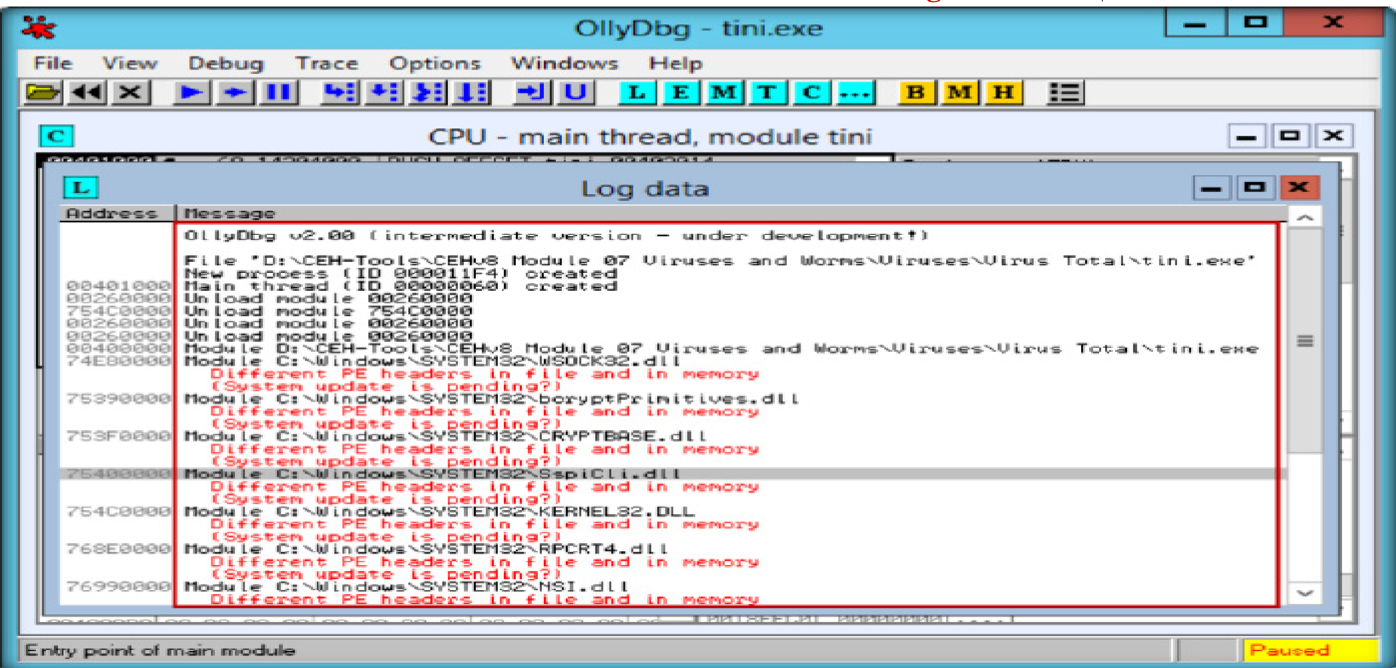
- كما نرى هذا والتي تمثل الشاشة الرئيسية لهذا التطبيق. والتي يمكنك من خلالها ادخال ملف البرمجيات الضارة التي تريد تحليلها وذلك من خلال النقر فوق **File** الموجود في شريط الأدوات العلوي ناحية اليسار ثم النقر فوق **Open**.



- بعض اختيار هذا التهديد لاختباره (**tini.exe**) نجد ان تحليل البرنامج له كالاتي:



- من خلال شريط الأدوات العلوي نقوم بالنقر فوق **View** ثم النقر فوق **LOG** او يمكننا اختصار ذلك بالنقر فقوى مفتاحي **Alt+L**.
- حيث ان هذا يستخدم لعرض بيانات **log** للملف **tini.exe** كالاتى:



- من خلال القائم المنسدلة من **VIEW** فيمكنك استخدام العديد من التنسيق حتى تختار منها ما تريده لرؤية البيانات التي تريدها مثل **Executable modules** و **Memory map** وغيرها.

Virus Analysis Tool: IDA Pro

المصدر: https://www.hex-rays.com/index.shtml

هي أداة Dissembler وdebugger الذي تدعم كل من الويندوز والينكس.

- **Dissembler**

Dissembler يعرض تنفيذ التعليمات للبرامج المختلفة في شكل رمزي، حتى إذا كان الرمز متاح في الشكل الثنائي. يعرض تنفيذ تعليمات المعالج في شكل خرائط. يتيح للمستخدمين لتحديد الفيروسات أيضا. على سبيل المثال، إن وجدت أن **screensaver** أو ملفات "**GIF**" تحاول التجسس على أي من التطبيقات الداخلية للمستخدم، فان **IDA Pro** يكشف هذا على الفور.

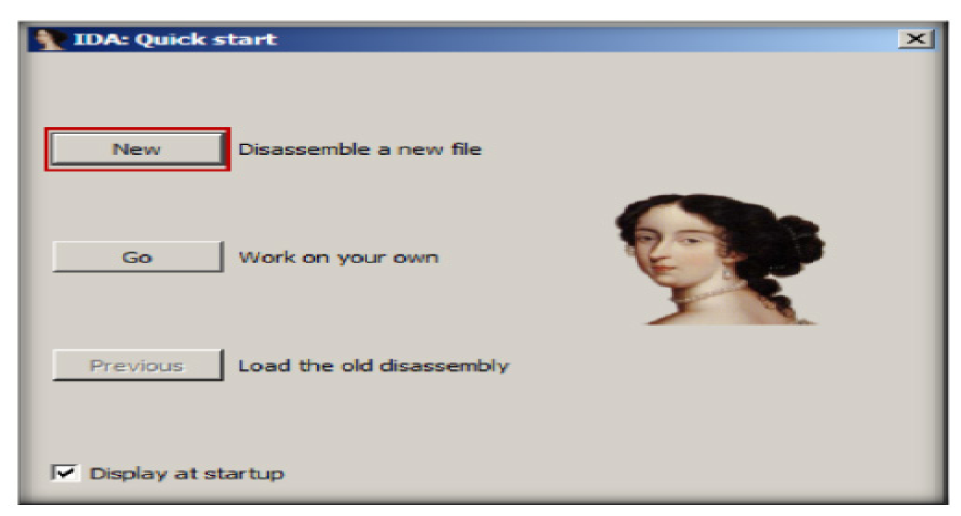
تم تطوير **IDA Pro** مع أحدث التقنيات التي تمكنها من تتبع الرموز الثنائية الصعبة ثم يعرضها على هيئة خرائط تنفيذيه قابله للقراءة.

- **Debugger**

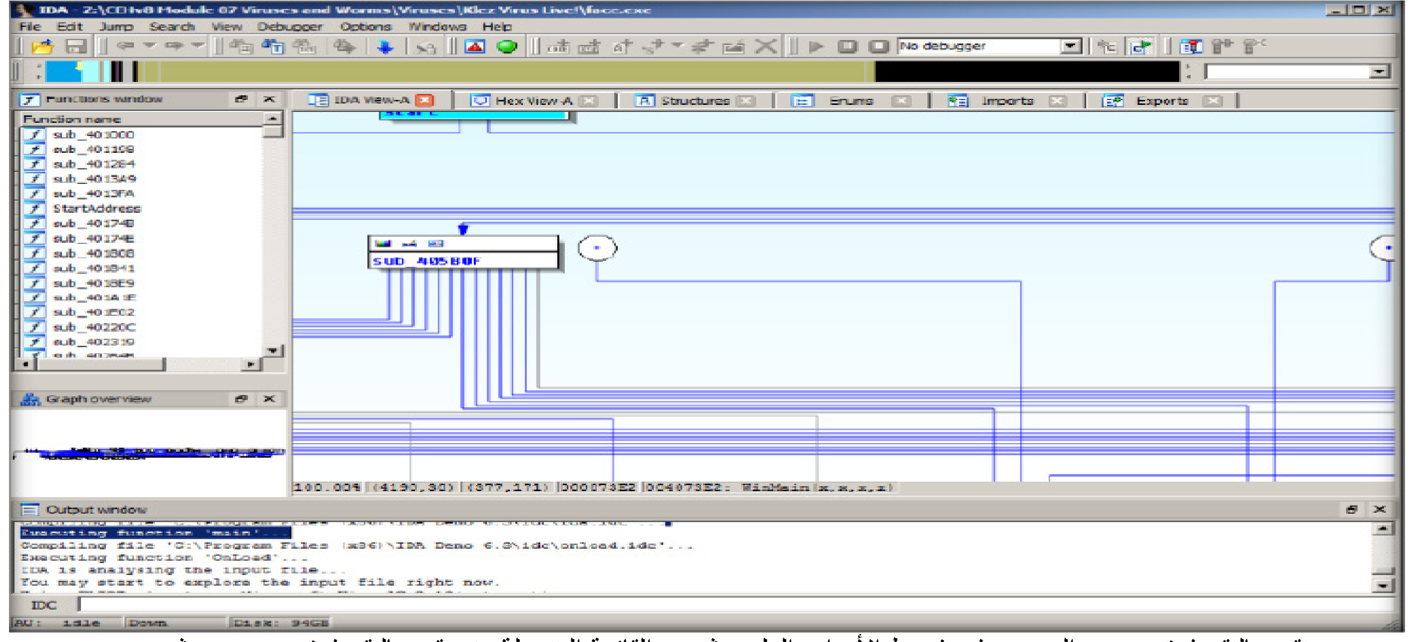
Debugger هو أداة تفاعلية والتي تكمل أداة **Dissembler** لأداء مهمة تحليل ساكنة (**static analysis**) في خطوة واحدة. فإنه يتجاوز عملية التشويش، مما يساعد **Dissembler** على معالجة الرموز المعادية بعمق.

IDA Pro هي الأداة التي تسمح لك لاستكشاف أي من انقطاعات في البرمجيات ونقاط الضعف ويتم استخدامه كانه مقاوم التلاعب (**tamper resistance**). هو اداة تفاعلية، مبرمجة، **Dissembler** متعدد العمليات إلى جانب **Debugger** سواء محلي وبعيدة ويضاف اليها بيئة كاملة من البرمجة المساعد. يمكن أيضا أن تستخدم هذا لحماية حقوق الخصوصية الأساسية الخاصة بك. ويستخدم هذا من قبل شركات مكافحة الفيروسات، وشركات الأبحاث، وشركات تطوير البرمجيات والوكالات والمنظمات العسكرية.

- نقوم بتثبيت البرنامج من خلال اتباع **wizard** الخاص بعملية التثبيت الى ان تظهر شاشة الترحيب التالية والتي نختار منها **new** كالاتي:

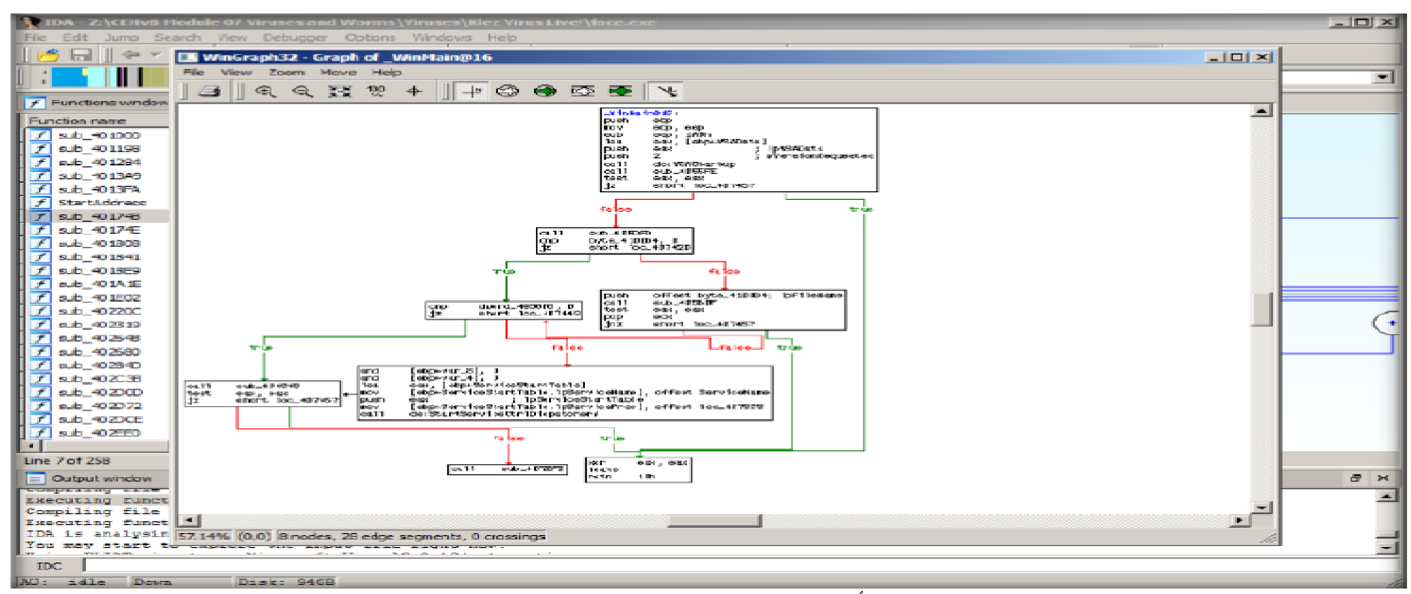


- هذا يؤدى أن يطلب منك اخيار التهديد الذي تريد ان تقوم بتحليليه، فنقوم بتحديد مكانه بالنسبة للبرنامج.
- ثم ننقر فوق **OK** ونفعل ذلك مع رسائل تحذيريه.
- بعد اختيار التهديد وعرضه بواسطة التطبيق فان الشاشة النهائية بعد تحليل التهديد تكون كالاتي:

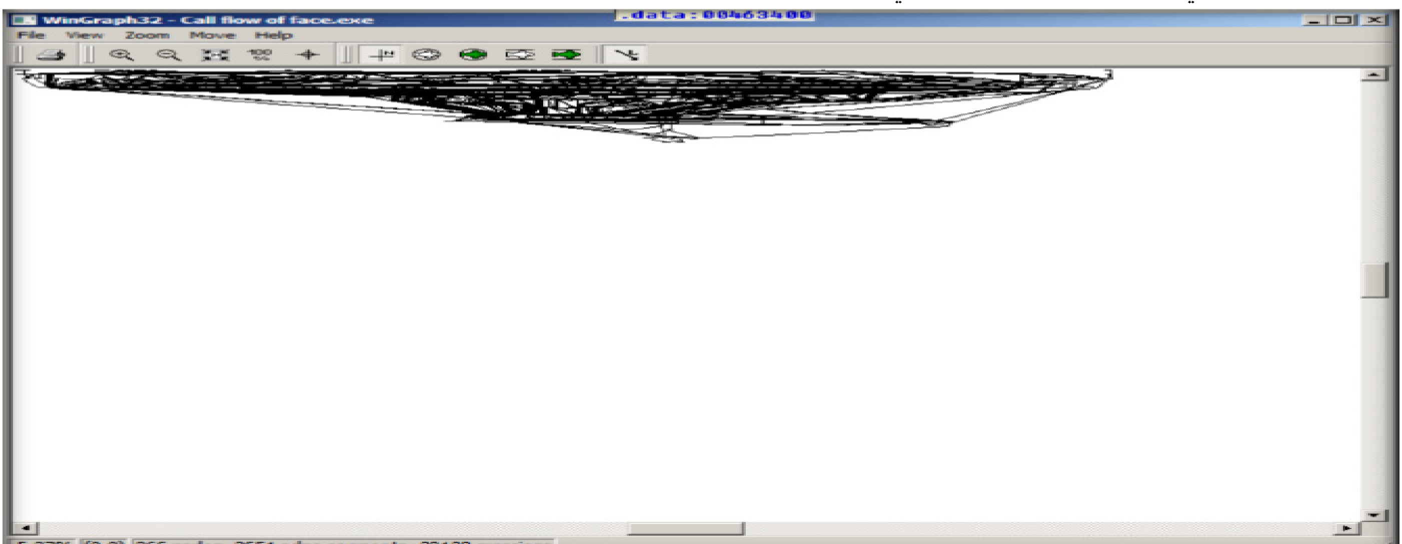


- نقوم بالنقر فوق **View** الموجود في شريط الأدوات العلوي ثم من القائمة المنسدلة منه نقوم بالنقر فوق **Graphs** ثم **Flow Chart**
- شاشة **Graphs** التي قمنا بالذهاب اليها سوف تظهر على النحو التالي: قم بتكبير (**zoom**)لترى بوضوح.

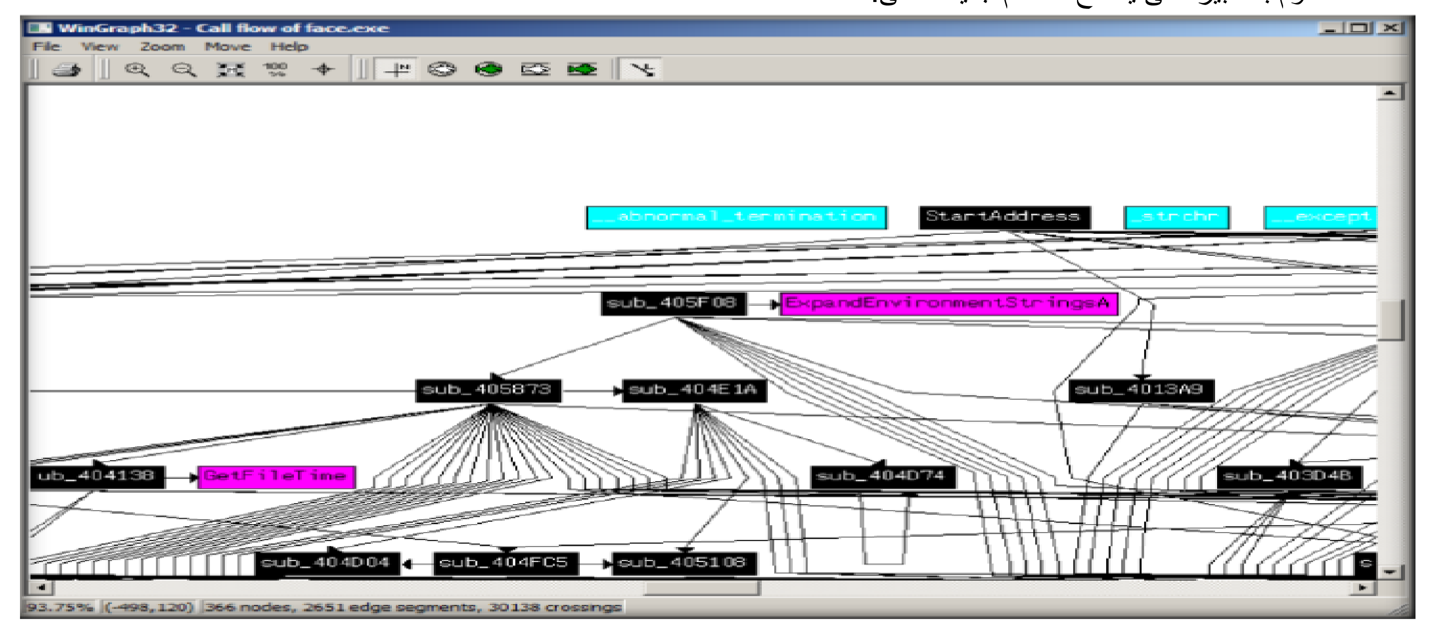




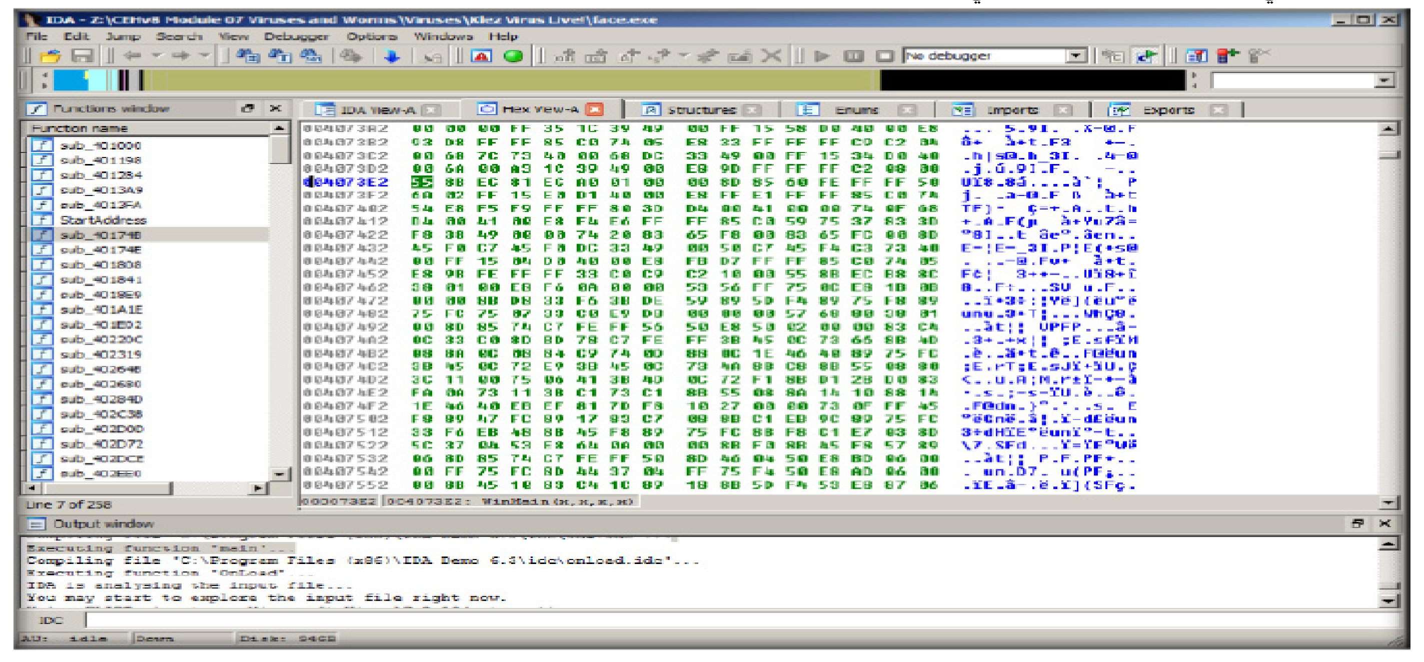
- نقوم بالنقر فوق **View** الموجود في شريط الأدوات العلوي ثم من القائمة المنسدلة منه نقوم بالنقر فوق **Graphs** ثم **Function call.** والتي تؤدى بالظهور بالشكل التالي.



- نقوم بالتكبير حتى يتضح المعالم جديا كالاتى:



- نقوم بالنقر فوق **Windows** الموجود في شريط الأدوات العلوي ثم من القائمة المنسدلة منه نقوم بالنقر فوق **Hex View-A.** والتي تؤدى بالظهور بالشكل التالي:



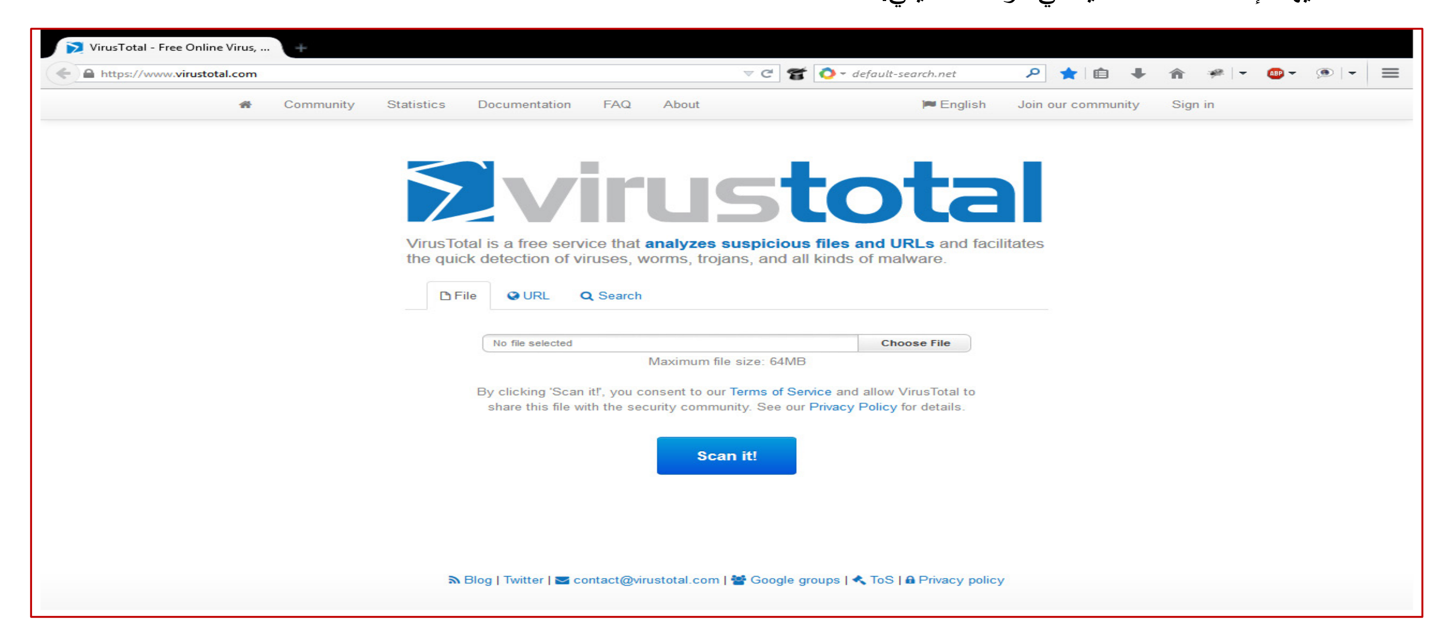
Online Malware Testing: VirusTotal

المصدر: https://www.virustotal.com

VirusTotalهي الخدمة التي تحلل الملفات المشبوهة ويسهل الكشف السريع عن الفيروسات والديدان وأحصنة طروادة، وجميع أنواع البرمجيات الخبيثة الكشف عنها بواسطة محركات مكافحة الفيروسات.

الميزات:

- خدمة مجانية ومستقلة.
- يستخدم محركات مكافحة الفيروسات متعددة.
- التحديثات التلقائية في الوقت الحقيقي لتواقيع الفيروسات.
- يعطي نتائج مفصلة من كل محرك مكافحة الفيروسات.
- لديها الإحصاءات العالمية في الوقت الحقيقي.



Online Malware Analysis Services

خدمات تحليل البرامج الضارة على الانترنت تسمح لك بفحص الملفات والموارد وتأمينها قبل هجوم المهاجمين وتقديم تنازلات لهم. وفيما يلي بعض الخدمات على الانترنت التي تقوم بتحليل البرامج الضارة على النحو التالي:

Anubis: Analyzing Unknown Binaries available at http://anubis.iseclab.org
Avast! Online Scanner available at http://onlinescan.avast.com
Malware Protection Center available at http://www.microsoft.com/en-in/default.aspx
ThreatExpert available at http://www.threatexpert.com
Dr. Web Online Scanners available at http://vms.drweb.com
Metascan Online available at http://www.metascan-online.com
Bitdefender QuickScan available at http://www.bitdefender.com
GFI SandBox available at http://www.gfi.com
UploadMalware.com available at http://www.uploadmalware.com
Fortinet available at http://www.fortiguard.com

7.5 التدابير المضادة (Countermeasures)

حتى الآن، لقد ناقشنا مختلف الفيروسات والديدان وتحليل البرامج الضارة. الآن سوف نناقش المضادات ليتم تطبيقها للحماية ضد الفيروسات والديدان، وإذا تم العثور على أي من هذه. وما التدابير المضادة التي تساعد في تعزيز الأمن. يبرز هذا القسم مختلف التدابير المضادة ضد الفيروسات والدودة.

طرق الكشف عن الفيروسات (Virus Detection Methods)

الفيروسات هو جزء هام من البرامج التي تكون مثبته على جهاز الكمبيوتر. إذا لم يكن هناك فاحص، إذا فهناك فرصة كبيرة أن يكون النظام قد ضرب من قبل الفيروسات ويعانون منهم. يجب تشغيل **virus protector** بشكل منتظم على جهاز الكمبيوتر، ومحرك الفحص وقاعدة بيانات تواقيع الفيروس يجب أن يتم تحديثها في كثير من الأحيان. برامج مكافحة الفيروسات لا جدوى منها إذا كان لا يعرف ما الذي تبحث عنه في أحدث الفيروسات. ينبغي للمرء أن يتذكر دائما أن برنامج مكافحة الفيروسات لا يمكن أن تتوقف كل شيء.

بحكم التجربة إذا كان البريد الإلكتروني يبدو وكأنه واحد مشبوهة(***suspicious one***) ، على سبيل المثال، إذا كان أحد لا يتوقع رسالة بريد الالكتروني من المرسل أو لا يعرف المرسل أو إذا كان رأس الرسالة يشبه شيئا تعرف أن المرسل لن يقوله عادة، يجب على المرء أن يكون حذرا حول فتح البريد الإلكتروني، كما قد يكون هناك خطر الإصابة بالعدوى عن طريق فيروس. الدودة **MyDoom** و **W32.Novarg.A@mm** تصيب العديد من مستخدمي الإنترنت في الآونة الأخيرة. هذه الديدان تصيب معظم المستخدمين من خلال البريد الإلكتروني.

أفضل الطرق الثلاث الأتية والتي تستخدم للكشف عن الفيروسات هي:

- فحص (scanning)
- التحقق من سلامة (Integrity checking)
- اعتراض (Interception)

بالإضافة إلى ذلك، يمكن لمزيج من بعض هذه التقنيات أن تكون أكثر فعالية.

الفحص (scanning)

- لحظة الكشف عن الفيروس في البرية، فان بائعي مكافحة الفيروسات في جميع أنحاء العالم يبدأ في كتابة برامج الفحص والتي تبحث عن سلاسل التواقيع (**signature strings**) (السمة المميزة للفيروس).
- يتم تحديد السلاسل واستخراجها من الفيروس عن طريق كاتبي الفاحص هؤلاء. مما أدى الى وجود فاحص جديد يبحث عن ملفات الذاكرة وقطاعات النظام عن سلاسل التواقيع الخاصة بالفيروس الجديد. الفاحص يعلن وجود الفيروس بمجرد أن يجد سلاسل التوقيع الذي يبحث عنه. حيث يمكن الكشف عن الفيروسات المعروفة فقط، والمحددة سابقا.

- كاتبي الفيروسات غالبا ما ينشأ العديد من الفيروسات الجديدة عن طريق تغيير الموجود. الفيروس الجديد، قد اتخذ بضع دقائق فقط لإنشائه. المهاجمين يقومون بإجراء تغييرات في كثير من الأحيان على الفيروسات القديمة للتخلص من الفاحص.
- بالإضافة إلى التعرف على التوقيع، فان الفاحص الجديد يستفيد من مختلف تقنيات الكشف الأخرى مثل تحليل الأكواد. قبل النظر الى خصائص اكواد الفيروس، فان الفاحص يختبر الأكواد الموجودة في مواقع مختلفة في الملف قابل للتنفيذ.
- في احتمال آخر، الفاحص ينشأ جهاز كمبيوتر وهمى (**virtual computer**) في ذاكرة الوصول العشوائي (**RAM**)واختبار البرامج عن طريق تنفيذها في الفضاء الوهمي. هذه التقنية، تدعى "**heuristic scanning**"، يمكن أيضا فحص الرسائل المسموحة التي قد تحتوي على فيروسات الكمبيوتر أو غيرها من المحتويات الغير مرغوب فيها.
- أهم مزايا الفاحص هي: (يمكنه أن يتحقق من البرامج قبل أن يتم إعدامهم -أسهل وسيلة للتحقق من البرامج الجديدة ضد أي فيروس معروف أو خبيث).
- **العوائق الرئيسية للفاحص هي:**
  - ❖ الفاحص القديم يمكن أن يكون غير موثوق به. وذلك نتيجة الزيادة الهائلة في الفيروسات الجديدة والتي تجعل يمكن الفاحص القديم سرعان ما يصبح بالي. فمن الأفضل استخدام أحدث الفواحص المتاحة في السوق.
  - ❖ حتى الفاحص الجديد لن يتم تجهيزه أبدا لكي يتعامل مع جميع التحديات الجديدة، لأن الفيروسات تظهر بسرعة أكبر مما يمكن تطوير فاحص جديد لمحاربة ذلك.

التحقق من سلامة (Integrity checking)

- منتجات فحص السلامة تؤدى وظائفها من خلال قراءة وتسجيل بيانات متكاملة لتطوير التوقيع أو خط أساسي لتلك الملفات وقطاعات النظام.
- منتجات فحص السلامة تتحقق من أي برنامج مدمج في الاستخبارات. هذا هو حقا الحل الوحيد الذي يمكن أن يأخذ الأهمية ضد جميع التهديدات على البيانات. يتم توفير وسيلة أكثر ثقة لمعرفة مقدار الضرر الذي قام به الفيروس عن طريق فاحص السلامة هذه، لأنه يمكن أن يتحقق من البيانات على أساس خط الأساس الذي أنشئت له أصلا.
- العيب من المدقق السلامة الأساسية هو أنه لا يمكن التفريق بين ملف فاسد ناجم عن خلل ومن ملف فاسد ناجم عن فيروس.
- مع ذلك، فان هناك بعض من محقق السلامة المتقدمة المتاحة التي هي قادرة على تحليل وتحديد أنواع التغييرات التي تحدثها الفيروسات. هناك عدد قليل من محقق السلامة والتي تجمع بين بعض تقنيات مكافحة الفيروسات مع التحقق من سلامة لخلق هجين. وهذا يبسط أيضا عملية فحص الفيروس.

اعتراض (Interception)

- الاستخدام الرئيسي **interception** هو لتشتيت قنابل المنطق وأحصنة طروادة.
- **Interception** تسيطر على الطلبات التي تذهب إلى نظام التشغيل للوصول إلى الشبكة أو من أجل بعض الإجراءات والتي تسبب خطرا على البرنامج. إذا وجد مثل هذا الطلب، فان **interception** عادة ما يعطى تنبيها بذلك ويسأل المستخدم إذا كان يريد لهذا الطلب المتابعة أم لا. لا توجد طرق يمكن الاعتماد عليها لاعتراض الفروع مباشرة لـ **low-level code** أو التعليمات المباشرة لمدخلات ومخرجات التعليمات بواسطة الفيروس.

في بعض الحالات، فإن الفيروس قادر على تعطيل برنامج الرصد نفسه. بالرجوع الى بضع سنوات الى الوراء فان الامر استغرق ثمانية بايت فقط من الأكواد لبرنامج مكافحة الفيروسات المستخدمة على نطاق واسع لإيقاف مهام الرصد الخاصة به.

التدابير المضادة ضد الفيروسات والديدان (Virus And Worms Countermeasures)

ينبغي اتباع التدابير الوقائية من أجل التقليل من إمكانية العدوى بالفيروس وفقدان البيانات. في حالة الالتزام بقواعد وإجراءات معينة، فإن إمكانية الوقوع ضحية لفيروس يمكن تقليلها. بعض من هذه الأساليب ما يلي:

- تثبيت برنامج مكافحة الفيروسات ليكتشف ويزيل الإصابات التي تظهر.
- تولد سياسة مكافحة الفيروسات للحوسبة آمنة وتوزيعه على الموظفين.
- إيلاء الاهتمام للتعليمات أثناء تنزيل الملفات أو أي برامج من الإنترنت.
- تحديث برامج مكافحة الفيروسات على أساس شهري، بحيث يمكن تحديد وتنظيف **bugs** جديدة.
- تجنب فتح المرفقات المستلمة من مرسل مجهول حيث تنتشر الفيروسات عبر مرفقات البريد الإلكتروني.
- عدوى فيروس يمكنها أن تتلف البيانات، وبالتالي يجب الحفاظ على بيانات احتياطية بانتظام.
- جدولة عمليات الفحص العادية لكافة محركات الأقراص بعد تثبيت برامج مكافحة الفيروسات.

- لا تقبل الأقراص أو البرامج دون فحصها الأولى باستخدام الإصدار الحالي من برنامج مكافحة الفيروسات.
- ضمان الموافقة على ارسال الأكواد القابلة للتنفيذ إلى المنظمة.
- تشغيل **disk clean up**، **registry scanner**، و **defragmentation** مرة واحدة في الأسبوع.
- لا تشغل الجهاز من قرص تمهيدي مصاب.
- قم بتشغيل جدار الحماية إذا كان نظام التشغيل المستخدم هو ويندوز **XP**.
- حافظ على المعرفة حول أحدث تهديدات الفيروسات.
- تشغيل مكافحة التجسس(**anti-spyware**) أو **adware** مرة واحدة في الأسبوع.
- التحقق من DVDS وCD5 من اصابتها بالفيروس.
- منع الملفات ذات أكثر من نوع من امتداد الملف.
- ضمان تشغيل حظر الإطارات المنبثقة (**pop-up blocker**) واستخدام جدار الحماية.
- كن حذرا مع الملفات التي يتم إرسالها عبر الرسائل الفورية.

Companion Antivirus: Immunet

المصدر: http://www.immunet.com/main/index.html

Companion Antivirus يعني أن **Immunet** متوافق مع حلول الحماية من الفيروسات الموجودة. **Immunet**يضيف، طبقة إضافية من الحماية خفيفة الوزن من أجل أكبر قطعه من العقل. منذ أصبحت حلول مكافحة الفيروسات التقليدية تكشف بالمتوسط 50٪ فقط من التهديدات على الإنترنت، فان معظم المستخدمين هم تحت حمايتها، وهذا هو السبب في ان كل جهاز كمبيوتر يمكن أن يستفيد من طبقة **Immunet** الأساسية للأمن.

Immunet يحمي قوة الكشف **ETHOS** و**SPERO**، **heuristics-based engine** و**cloud engine**. مستخدمي النسخة الزائدة يستفادوا من محرك ثالث يسمى **TETRA**، والذي يوفر الحماية عندما لا تكون متصلا بالإنترنت.



أدوات مكافحة الفيروسات

أدوات مكافحة الفيروسات تمنع وتكشف وتزيل الفيروسات والأكواد الخبيثة الأخرى من النظام الخاص بك. هذه الأدوات تقوم بحماية النظام الخاص بك وإصلاح الفيروسات في جميع رسائل البريد الإلكتروني الواردة والصادرة ومرفقات الرسائل الفورية. بالإضافة إلى ذلك، هذه الأدوات تقوم بمراقبة حركة مرور الشبكة للأنشطة الخبيثة. وفيما يلي بعض أدوات مكافحة الفيروسات التي يمكن استخدامها لغرض الكشف وقتل الفيروسات في النظم على النحو التالي:

AVG Antivirus available at http://free.avg.com
BitDefender available at http://www.bitdefender.com
Kaspersky Anti-Virus available at http://www.kaspersky.com
Trend Micro Internet Security Pro available at http://apac.trendmicro.com
Norton Anti-Virus available at http://www.symantec.com
F-Secure Anti-Virus available at http://www.f-secure.com
Avast Pro Antivirus available at http://www.avast.com
McAfee Anti-Virus Plus 2013 available at http://home.mcafee.com
ESET Smart Security 5 available at http://www.eset.com
Total Defense Internet Security Suite available at http://www.totaldefense.com

7.6 مختبري الاختراق (PENETRATION TEST)

يجب إجراء اختبار الاختراق ضد الفيروسات والديدان، لأنها هي الوسيلة الأكثر استخداما على نطاق واسع للهجوم. أنها لا تتطلب معرفة واسعة للاستخدام. وبالتالي، يجب إجراء اختبار الاختراق على النظام الخاص بك أو الشبكة قبل ان يستغلها المهاجم الحقيقي.
يوفر هذا القسم نظرة ثاقبة على اختبار الاختراق ضد الفيروسات والدودة.

منذ أن اصبحت هاكر أخلاقي وخبير في أداء اختبار الاختراق، حيث يكلفك مدير تكنولوجيا المعلومات لاختبار الشبكة ضد أي من الفيروسات والديدان التي يمكن أن تتلف أو تسرق معلومات المنظمة. تحتاج لبناء الفيروسات والديدان ثم تحاول ضخها في شبكة وهمية (الجهاز الوهمي) وتتحقق ما إذا كان يتم الكشف عنها من قبل برامج مكافحة الفيروسات أو قادرة على تجاوز جدار حماية الشبكة. بمثابة إنك مختبر اختراق، يجب تنفيذ الخطوات التالية لإجراء اختبار الاختراق ضد الفيروسات:

- **الخطوة 1: تثبيت برنامج مكافحة الفيروسات**

يجب تثبيت برنامج مكافحة الفيروسات على البنية التحتية للشبكة وعلى النظام للمستخدم النهائي قبل إجراء اختبار الاختراق.

- **الخطوة 2: تحديث برامج مكافحة الفيروسات**

تحقق ما إذا كان يتم تحديث برامج مكافحة الفيروسات الخاص بك أم لا. إن لم يكن فقم بتحديث برامج مكافحة الفيروسات.

- **الخطوة 3: فحص النظام بحثا عن الفيروسات**

يجب أن تحاول فحص النظام التي تستهدفه؛ هذا سوف يساعدك على إصلاح الضرر أو حذف الملفات المصابة بالفيروسات.

- **الخطوة 4: تعيين مكافحة الفيروسات لعزل أو حذف الفيروس**

إعداد برنامج مكافحة الفيروسات الخاص بك لمقارنة محتويات الملف مع توقيعات فيروس الكمبيوتر المعروف، وتحديد الملفات المصابة، والحجر الصحي وإصلاحهم إذا كان ذلك ممكنا، أو حذفها إن لم يكن.

- **الخطوة 5: الذهاب إلى الوضع الآمن (safe mode) وحذف الملف المصابة يدويا**

إذا لم يتم إزالة الفيروس، فانتقل إلى الوضع الآمن (**safe mode**) وقم بحذف الملف المصاب يدويا.

- **الخطوة 6: فحص النظام عن العمليات الجارية**

يجب فحص النظام الخاص بك ضد أي عملية مشبوهة تم تشغيلها. يمكنك القيام بذلك باستخدام أدوات مثل **What's Running**، **HijackThis**، الخ.

- **الخطوة 7: تفحص النظام عن إدخالات registry المشبوهة.**

يجب فحص النظام الخاص بك عن إدخالات **registry** المشبوهة. يمكنك القيام بذلك باستخدام أدوات مثل **JV Power Tools** و**Regshot**.

- **الخطوة 8: تفحص النظام عن خدمات الويندوز المشبوهة**

يجب فحص خدمات الويندوز المشبوهة التي تعمل على النظام الخاص بك. يمكنك القيام بذلك باستخدام أدوات مثل **SrvMan** و**ServiWin**.

- **الخطوة 9: فحص النظام عن برامج بدء التشغيل المشبوهة**

يجب فحص النظام الخاص بك عن برامج بدء التشغيل المشبوهة التي تعمل على النظام الخاص بك. باستخدام أدوات مثل **Starter**، **Security AutoRun**، و **Autoruns** يمكن استخدامها لفحص برامج بدء التشغيل.

- **الخطوة 10: فحص النظام عن سلامة الملفات والمجلدات**

عليك أن تفحص النظام الخاص للتحقق من سلامة الملفات والمجلدات. يمكنك القيام بذلك باستخدام أدوات مثل **FCIV**، **TRIPWIRE**، و**SIGVERIF**.

- **الخطوة 11: فحص النظام عن تعديلات نظام التشغيل الحرجة**

يمكنك فحص التعديلات أو التلاعب بملفات نظام التشغيل الحرجة باستخدام أدوات مثل **TRIPWIRE** أو مقارنة قيم الهاش يدويا إذا كان لديك نسخة احتياطية.

- **الخطوة 12: وثيقة عن النتائج**

يمكن لهذه النتائج أن تساعدك على تحديد الإجراء التالي إذا تم تحديد الفيروسات على النظام.

- **الخطوة 13: عزل النظام المصاب**

بمجرد أن يتم تحديد النظام المصاب، فيجب عزل النظام المصاب عن الشبكة فورا من أجل منع المزيد من الإصابة.

- **الخطوة 14: تطهير النظام المصابة بأكمله**

يجب إزالة العدوى بالفيروس من النظام الخاص بك باستخدام أحدث برامج مكافحة الفيروسات المحدثة.

الحمد لله تعالى، وبحول الله تعالى نكون قد انتهينا من الوحدة السادسة ونلقاكم مع الوحدة التالية:

د. محمد صبحي طيبه